

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-015530

(43)Date of publication of application : 15.01.2004

(51)Int.Cl.

H04L 12/66
G06F 15/00
G09C 1/00
H04L 9/32
H04L 12/46
H04L 12/56

(21)Application number : 2002-167516

(71)Applicant : SONY CORP

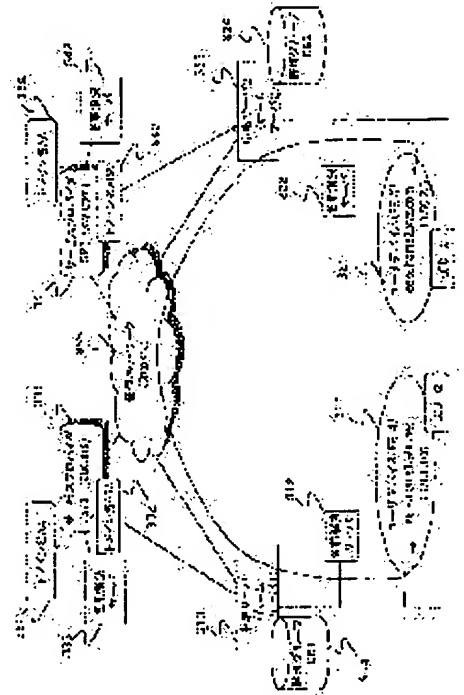
(22)Date of filing : 07.06.2002

(72)Inventor : OKA MAKOTO
SHIMADA NOBORU
KAWAGUCHI TAKAYOSHI
MASUGI MADOKA
ISHIBASHI YOSHITO
ABE HIROSHI
TOYOSHIMA NOBUTAKA

(54) ACCESS RIGHT MANAGEMENT SYSTEM, RELAY SERVER AND METHOD THEREFOR, AS WELL AS COMPUTER PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a system and a method for performing access restriction surely in communication through network.
SOLUTION: As to communication among communication processing units through communication network, a relay server like a home server implements verification and examination of an attribute certificate of an access originator. The access originator implements determination processing of whether the accessing originator belongs to an authorized member of the access opponent. Only when the access originator belongs to the permitted one by the access opponent, name resolution processing is implemented, and address information of the access opponent is notified to the access originator. A group attribute certificate describing a domain name and a host name of the access originator is referred to, and update of address corresponding to the domain name and the host name is implemented in this constitution.



LEGAL STATUS

[Date of request for examination]

10.05.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

【特許請求の範囲】

【請求項 1】

通信ネットワークを介した通信処理装置間の通信におけるアクセス権限管理システムであり、
アクセス先通信処理装置のホスト名とアドレスの対応データを有し、アクセス先通信処理装置に対応するホスト名に関する名前解決処理を実行する名前解決サーバと、
アクセス元通信処理装置から、アクセス先通信処理装置のホスト名を受信するとともに、
特定通信処理装置の集合からなるグループに対応して設定されるグループ識別情報を格納し発行者電子署名を有するグループ属性証明書を受信し、該グループ属性証明書の検証処理、および、アクセス先通信処理装置のアクセス許容グループにアクセス元通信処理装置
10
が属するか否かの審査処理を実行し、該検証および審査が成立したことを条件として、前記名前解決サーバを適用した名前解決処理により、アクセス先通信処理装置のアドレスを取得し、前記アクセス元通信処理装置に対する通知処理を実行する中継サーバと、
を有することを特徴とするアクセス権限管理システム。

【請求項 2】

前記グループ属性証明書は、
ドメイン名をグループ識別情報として格納し、
前記中継サーバは、
前記アクセス先通信処理装置に対するアクセス許可グループ情報としてドメイン名による
アクセス許可グループ情報を格納した許可グループデータベースを参照して、アクセス先
20
通信処理装置のアクセス許容グループにアクセス元通信処理装置が属するか否かの審査処理を実行する構成であることを特徴とする請求項 1 に記載のアクセス権限管理システム。

【請求項 3】

前記グループ属性証明書は、
ホスト名をグループ識別情報として格納し、
前記中継サーバは、
前記アクセス先通信処理装置に対するアクセス許可グループ情報としてホスト名による
アクセス許可グループ情報を格納した許可グループデータベースを参照して、アクセス先通
信処理装置のアクセス許容グループにアクセス元通信処理装置が属するか否かの審査処理
を実行する構成であることを特徴とする請求項 1 に記載のアクセス権限管理システム。 30

【請求項 4】

前記中継サーバは、
前記アクセス先通信処理装置にネットワーク接続されたホームサーバであることを特徴とする請求項 1 に記載のアクセス権限管理システム。

【請求項 5】

前記中継サーバは、
前記アクセス先通信処理装置に対応するドメイン名またはホスト名に対応するアドレスの更新処理を実行する構成を有し、
前記アクセス先通信処理装置の有する属性証明書の検証の成立を条件として前記更新処理
を実行する構成であることを特徴とする請求項 1 に記載のアクセス権限管理システム。 40

【請求項 6】

前記中継サーバは、
アクセス元通信処理装置との相互認証を実行し、相互認証の成立を条件として、前記アクセス元通信処理装置から提示されるグループ属性証明書の検証および審査を実行する構成であることを特徴とする請求項 1 に記載のアクセス権限管理システム。

【請求項 7】

前記グループ属性証明書は、グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、
前記中継サーバは、
前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書 50

の検証を併せて実行する構成であることを特徴とする請求項 1 に記載のアクセス権限管理システム。

【請求項 8】

通信ネットワークを介した通信処理装置間の通信におけるアクセス権限管理を実行する中継サーバであり、
アクセス元通信処理装置から、アクセス先通信処理装置のホスト名を受信するとともに、特定通信処理装置の集合からなるグループに対応して設定されるグループ識別情報を格納し、発行者電子署名を有するグループ属性証明書を受信し、該グループ属性証明書の検証処理、および、アクセス先通信処理装置のアクセス許容グループにアクセス元通信処理装置が属するか否かの審査処理を実行し、該検証および審査が成立したことを条件として、名前解決サーバを適用した名前解決処理により、アクセス先通信処理装置のアドレスを取得し、前記アクセス元通信処理装置に対する通知処理を実行する構成を有することを特徴とする中継サーバ。 10

【請求項 9】

前記グループ属性証明書は、
ドメイン名をグループ識別情報として格納し、
前記中継サーバは、
前記アクセス先通信処理装置に対するアクセス許可グループ情報としてドメイン名によるアクセス許可グループ情報を格納した許可グループデータベースを参照して、アクセス先通信処理装置のアクセス許容グループにアクセス元通信処理装置が属するか否かの審査処理を実行する構成であることを特徴とする請求項 8 に記載の中継サーバ。 20

【請求項 10】

前記グループ属性証明書は、
ホスト名をグループ識別情報として格納し、
前記中継サーバは、
前記アクセス先通信処理装置に対するアクセス許可グループ情報としてホスト名によるアクセス許可グループ情報を格納した許可グループデータベースを参照して、アクセス先通信処理装置のアクセス許容グループにアクセス元通信処理装置が属するか否かの審査処理を実行する構成であることを特徴とする請求項 8 に記載の中継サーバ。 30

【請求項 11】

前記中継サーバは、
前記アクセス先通信処理装置にネットワーク接続されたホームサーバであることを特徴とする請求項 8 に記載の中継サーバ。

【請求項 12】

前記中継サーバは、
前記アクセス先通信処理装置に対応するドメイン名またはホスト名に対応するアドレスの更新処理を実行する構成を有し、
前記アクセス先通信処理装置の有する属性証明書の検証の成立を条件として前記更新処理を実行する構成であることを特徴とする請求項 8 に記載の中継サーバ。 40

【請求項 13】

前記中継サーバは、
アクセス元通信処理装置との相互認証を実行し、相互認証の成立を条件として、前記アクセス元通信処理装置から提示されるグループ属性証明書の検証および審査を実行する構成であることを特徴とする請求項 8 に記載の中継サーバ。

【請求項 14】

前記グループ属性証明書は、グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、
前記中継サーバは、
前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書の検証を併せて実行する構成であることを特徴とする請求項 8 に記載の中継サーバ。 50

【請求項 15】

通信ネットワークを介した通信処理装置間の通信におけるアクセス権限管理方法であり、中継サーバにおいて、アクセス元通信処理装置から、アクセス先通信処理装置のホスト名を受信するとともに、特定通信処理装置の集合からなるグループに対応して設定されるグループ識別情報を格納し発行者電子署名を有するグループ属性証明書を受信するステップ

、
該グループ属性証明書の検証処理、および、アクセス先通信処理装置のアクセス許容グループにアクセス元通信処理装置が属するか否かの審査処理を実行するステップ、
該検証および審査が成立したことを条件として、名前解決サーバを適用した名前解決処理により、アクセス先通信処理装置のアドレスを取得し、前記アクセス元通信処理装置に対する通知処理を実行するステップ、
を含むことを特徴とするアクセス権限管理方法。

【請求項 16】

前記グループ属性証明書は、
ドメイン名をグループ識別情報として格納し、
前記中継サーバは、
前記アクセス先通信処理装置に対するアクセス許可グループ情報としてドメイン名によるアクセス許可グループ情報を格納した許可グループデータベースを参照して、アクセス先通信処理装置のアクセス許容グループにアクセス元通信処理装置が属するか否かの審査処理を実行することを特徴とする請求項 15 に記載のアクセス権限管理方法。

【請求項 17】

前記グループ属性証明書は、
ホスト名をグループ識別情報として格納し、
前記中継サーバは、
前記アクセス先通信処理装置に対するアクセス許可グループ情報としてホスト名によるアクセス許可グループ情報を格納した許可グループデータベースを参照して、アクセス先通信処理装置のアクセス許容グループにアクセス元通信処理装置が属するか否かの審査処理を実行することを特徴とする請求項 15 に記載のアクセス権限管理方法。

【請求項 18】

前記中継サーバは、
前記アクセス先通信処理装置にネットワーク接続されたホームサーバであることを特徴とする請求項 15 に記載のアクセス権限管理方法。

【請求項 19】

前記アクセス権限管理方法において、前記中継サーバは、さらに、
前記アクセス先通信処理装置に対応するドメイン名またはホスト名に対応するアドレスの更新処理を実行するステップを有し、
前記アクセス先通信処理装置の有する属性証明書の検証の成立を条件として前記更新処理を実行することを特徴とする請求項 15 に記載のアクセス権限管理方法。

【請求項 20】

前記中継サーバは、
アクセス元通信処理装置との相互認証を実行し、相互認証の成立を条件として、前記アクセス元通信処理装置から提示されるグループ属性証明書の検証および審査を実行することを特徴とする請求項 15 に記載のアクセス権限管理方法。

【請求項 21】

前記グループ属性証明書は、グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、
前記中継サーバは、
前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書の検証を併せて実行することを特徴とする請求項 15 に記載のアクセス権限管理方法。

【請求項 22】

通信ネットワークを介した通信処理装置間の通信におけるアクセス権限管理処理を実行せしめるコンピュータ・プログラムであって、
アクセス元通信処理装置から、アクセス先通信処理装置のホスト名を受信するとともに、特定通信処理装置の集合からなるグループに対応して設定されるグループ識別情報を格納し発行者電子署名を有するグループ属性証明書を受信するステップ、
該グループ属性証明書の検証処理、および、アクセス先通信処理装置のアクセス許容グループにアクセス元通信処理装置が属するか否かの審査処理を実行するステップ、
該検証および審査が成立したことを条件として、名前解決サーバを適用した名前解決処理により、アクセス先通信処理装置のアドレスを取得し、前記アクセス元通信処理装置に対する通知処理を実行するステップ、
を有することを特徴とするコンピュータ・プログラム。

10

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、アクセス権限管理システム、中継サーバ、および方法、並びにコンピュータ・プログラムに関する。例えば特定の通信端末、あるいはユーザにのみアクセス権限を付与し、アクセス権限を有する機器あるいはユーザからのアクセスのみを許容可能としたアクセス権限管理システム、中継サーバ、および方法、並びにコンピュータ・プログラムに関する。

【0002】

20

【従来の技術】

昨今、インターネット等の通信ネットワークを介した通信が盛んに行なわれている。ネットワークに接続されている機器は、アドレスによって通信先が特定され、相互の通信が可能となる。インターネットではルーティングプロトコルとしてIP (Internet Protocol) が用いられている。現在主に使用されているIPはIPv4であり、発信元/宛先として32ビットからなるアドレス (IPアドレス) が用いられている。インターネット通信においては、32ビットIPアドレスを各発信元/宛先にユニークに割り当てるグローバルIPアドレスを採用し、IPアドレスに応じて、個々の発信元/宛先を判別している。

【0003】

30

IPアドレス (IPv4) は32ビットのアドレスを8ビットを単位として10進数で表して表記する。このような数字の羅列はユーザにとっては覚えにくいものである。このため、IPアドレスの代わりにホストネームを用いて通信を可能とするためのDNS (Domain Name System) が利用される。

【0004】

DNSサーバが端末 (ホスト) のIPアドレスとホスト名の対応付けを管理し、端末が通信を行うときにDNSサーバにアクセスしてホスト名に基づいてホストアドレス (IPアドレス) を得ることができる。

【0005】

すなわち、アドレスは単なるビット列であるので、これを利用者が直接管理することは困難である。そのため、インターネットにおいては人が理解しやすい名前を付与し、それをアドレスに変換する機構としてDNS (Domain Name System) が導入されている。

40

【0006】

WWWやコンテンツ配信サービス等ではサーバと呼ばれるサービスの提供を専門に行う機器に利用者がアクセスすることが多いのに対し、利用者同士でチャットを行うインスタント・メッセージングといった場合では、利用者の機器を直接接続する形態がとられることがある。この直接接続形態を一般的に「ピア・ツー・ピア」 (Peer to Peer) と呼ぶ。

【0007】

50

情報処理装置間の直接通信処理としてのピア・ツー・ピア (P2P: Peer-to-Peer) ネットワークとは、集中的に処理を行なうサーバを設置するのではなく、各ネットワーククライアントが持つ資源としての情報処理装置、例えばPC、携帯端末、PDA、携帯電話、さらに、通信処理可能な機能を持つあるいは通信機器間を直接接続した通信ネットワークである。

【0008】

ピア・ツー・ピア (P2P: Peer-to-Peer) ネットワーク技術は、米IBM社が提唱するAPPN (Advanced Peer to Peer Networking) の中で用いられたのが最初とされている。このネットワークを使うことで、従来のようなクライアント-サーバ型ネットワークにおいてコンテンツ配信を行う場合に必要となる巨大な配信サーバを設置する必要がなくなり、各ネットワーククライアントが持つ資源に分散配置されたコンテンツを多くのユーザが利用可能となり、大容量のコンテンツの分散格納および、配信が可能となる。

【0009】

【発明が解決しようとする課題】

しかし、特定のサービスプロバイダによるコンテンツ配信等の場合は、一般的に配信を行うサービスプロバイダと利用者とはあらかじめ契約等で信頼関係を構築し、データ送信側と受信側とが、契約に基づく信頼関係をベースとしたデータ送受信が可能であるのに対し、リモートコントロールやインスタント・メッセージングでは、特に信頼関係のない不特定多数から各クライアントの通信端末に対するアクセス要求があり、データの送受信が実行されることになる。

【0010】

従って、インターネット等に接続した通信処理装置としてのクライアント端末は、クライアント端末や、そのクライアント端末を接続したホームネットワークに対して悪意を持った他のネットワーク接続機器からDoS (Denial of Service) 攻撃等の通信妨害を受ける可能性がある。DoS (Denial of Service) 攻撃とは、大量のデータや不正パケット、あるいはコマンドを送信することにより、サービスの提供を困難とさせるものである。

【0011】

たとえ一度信頼関係を結んだ通信端末間であっても、その信頼関係を解消した場合、アドレスが固定アドレスであると、引き続きアクセスを実行することが可能となってしまう、不正アクセスや攻撃の可能な状態が維持されてしまうといった問題がある。

【0012】

本発明は、上記問題点を鑑みてなされたものであり、ネットワークに接続されたクライアント端末等、通信処理装置に対する不正なアクセスを排除する構成を提供するものである。

【0013】

本発明は、PC、携帯端末、PDA、携帯電話等のクライアント端末としての通信処理装置の許容するユーザあるいは端末からのアクセス要求のみを許可する構成を実現するアクセス権限管理システム、中継サーバ、および方法、並びにコンピュータ・プログラムを提供することを目的とする。

【0014】

さらに、具体的には、本発明は、安全なホームネットワークの実現に向けて、DoS (Denial of Service) 攻撃等への対策を考慮したものであり、ネットワークに接続された例えばホームサーバにおいて、アクセス要求元から提示される属性証明書を適用したアクセス権限の確認処理を実行し、アクセス権限の確認を条件として名前解決処理を実行する構成として、アクセスを許容したユーザあるいは端末からの要求に対してのみアクセスを許容することを可能としたアクセス権限管理システム、中継サーバ、および方法、並びにコンピュータ・プログラムを提供することを目的とする。

【0015】

【課題を解決するための手段】

本発明の第1の側面は、
通信ネットワークを介した通信処理装置間の通信におけるアクセス権限管理システムであり、
アクセス先通信処理装置のホスト名とアドレスの対応データを有し、アクセス先通信処理装置に対応するホスト名に関する名前解決処理を実行する名前解決サーバと、
アクセス元通信処理装置から、アクセス先通信処理装置のホスト名を受信するとともに、
特定通信処理装置の集合からなるグループに対応して設定されるグループ識別情報を格納し発行者電子署名を有するグループ属性証明書を受信し、該グループ属性証明書の検証処理、および、アクセス先通信処理装置のアクセス許容グループにアクセス元通信処理装置が属するか否かの審査処理を実行し、該検証および審査が成立したことを条件として、前記名前解決サーバを適用した名前解決処理により、アクセス先通信処理装置のアドレスを取得し、前記アクセス元通信処理装置に対する通知処理を実行する中継サーバと、
を有することを特徴とするアクセス権限管理システムにある。

【0016】

さらに、本発明のアクセス権限管理システムの一実施態様において、前記グループ属性証明書は、ドメイン名をグループ識別情報として格納し、前記中継サーバは、前記アクセス先通信処理装置に対するアクセス許可グループ情報としてドメイン名によるアクセス許可グループ情報を格納した許可グループデータベースを参照して、アクセス先通信処理装置のアクセス許容グループにアクセス元通信処理装置が属するか否かの審査処理を実行する構成であることを特徴とする。

【0017】

さらに、本発明のアクセス権限管理システムの一実施態様において、前記グループ属性証明書は、ホスト名をグループ識別情報として格納し、前記中継サーバは、前記アクセス先通信処理装置に対するアクセス許可グループ情報としてホスト名によるアクセス許可グループ情報を格納した許可グループデータベースを参照して、アクセス先通信処理装置のアクセス許容グループにアクセス元通信処理装置が属するか否かの審査処理を実行する構成であることを特徴とする。

【0018】

さらに、本発明のアクセス権限管理システムの一実施態様において、前記中継サーバは、前記アクセス先通信処理装置にネットワーク接続されたホームサーバであることを特徴とする。

【0019】

さらに、本発明のアクセス権限管理システムの一実施態様において、前記中継サーバは、前記アクセス先通信処理装置に対応するドメイン名またはホスト名に対応するアドレスの更新処理を実行する構成を有し、前記アクセス先通信処理装置の有する属性証明書の検証の成立を条件として前記更新処理を実行する構成であることを特徴とする。

【0020】

さらに、本発明のアクセス権限管理システムの一実施態様において、前記中継サーバは、アクセス元通信処理装置との相互認証を実行し、相互認証の成立を条件として、前記アクセス元通信処理装置から提示されるグループ属性証明書の検証および審査を実行する構成であることを特徴とする。

【0021】

さらに、本発明のアクセス権限管理システムの一実施態様において、前記グループ属性証明書は、グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、前記中継サーバは、前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書の検証を併せて実行する構成であることを特徴とする。

【0022】

さらに、本発明の第2の側面は、
通信ネットワークを介した通信処理装置間の通信におけるアクセス権限管理を実行する中

継サーバであり、アクセス元通信処理装置から、アクセス先通信処理装置のホスト名を受信するとともに、特定通信処理装置の集合からなるグループに対応して設定されるグループ識別情報を格納し発行者電子署名を有するグループ属性証明書を受信し、該グループ属性証明書の検証処理、および、アクセス先通信処理装置のアクセス許容グループにアクセス元通信処理装置が属するか否かの審査処理を実行し、該検証および審査が成立したことを条件として、名前解決サーバを適用した名前解決処理により、アクセス先通信処理装置のアドレスを取得し、前記アクセス元通信処理装置に対する通知処理を実行する構成を有することを特徴とする中継サーバにある。

【0023】

10

さらに、本発明の中継サーバの一実施態様において、前記グループ属性証明書は、ドメイン名をグループ識別情報として格納し、前記中継サーバは、前記アクセス先通信処理装置に対するアクセス許可グループ情報としてドメイン名によるアクセス許可グループ情報を格納した許可グループデータベースを参照して、アクセス先通信処理装置のアクセス許容グループにアクセス元通信処理装置が属するか否かの審査処理を実行する構成であることを特徴とする。

【0024】

さらに、本発明の中継サーバの一実施態様において、前記グループ属性証明書は、ホスト名をグループ識別情報として格納し、前記中継サーバは、前記アクセス先通信処理装置に対するアクセス許可グループ情報としてホスト名によるアクセス許可グループ情報を格納した許可グループデータベースを参照して、アクセス先通信処理装置のアクセス許容グループにアクセス元通信処理装置が属するか否かの審査処理を実行する構成であることを特徴とする。

20

【0025】

さらに、本発明の中継サーバの一実施態様において、前記中継サーバは、前記アクセス先通信処理装置にネットワーク接続されたホームサーバであることを特徴とする。

【0026】

さらに、本発明の中継サーバの一実施態様において、前記中継サーバは、前記アクセス先通信処理装置に対応するドメイン名またはホスト名に対応するアドレスの更新処理を実行する構成を有し、前記アクセス先通信処理装置の有する属性証明書の検証の成立を条件として前記更新処理を実行する構成であることを特徴とする。

30

【0027】

さらに、本発明の中継サーバの一実施態様において、前記中継サーバは、アクセス元通信処理装置との相互認証を実行し、相互認証の成立を条件として、前記アクセス元通信処理装置から提示されるグループ属性証明書の検証および審査を実行する構成であることを特徴とする。

【0028】

さらに、本発明の中継サーバの一実施態様において、前記グループ属性証明書は、グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、前記中継サーバは、前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書の検証を併せて実行する構成であることを特徴とする。

40

【0029】

さらに、本発明の第3の側面は、通信ネットワークを介した通信処理装置間の通信におけるアクセス権限管理方法であり、中継サーバにおいて、アクセス元通信処理装置から、アクセス先通信処理装置のホスト名を受信するとともに、特定通信処理装置の集合からなるグループに対応して設定されるグループ識別情報を格納し発行者電子署名を有するグループ属性証明書を受信するステップ、該グループ属性証明書の検証処理、および、アクセス先通信処理装置のアクセス許容グループにアクセス元通信処理装置が属するか否かの審査処理を実行するステップ、

50

該検証および審査が成立したことを条件として、名前解決サーバを適用した名前解決処理により、アクセス先通信処理装置のアドレスを取得し、前記アクセス元通信処理装置に対する通知処理を実行するステップ、
を含むことを特徴とするアクセス権限管理方法にある。

【0030】

さらに、本発明のアクセス権限管理方法の一実施態様において、前記グループ属性証明書は、ドメイン名をグループ識別情報として格納し、前記中継サーバは、前記アクセス先通信処理装置に対するアクセス許可グループ情報としてドメイン名によるアクセス許可グループ情報を格納した許可グループデータベースを参照して、アクセス先通信処理装置のアクセス許可グループにアクセス元通信処理装置が属するか否かの審査処理を実行すること
を特徴とする。 10

【0031】

さらに、本発明のアクセス権限管理方法の一実施態様において、前記グループ属性証明書は、ホスト名をグループ識別情報として格納し、前記中継サーバは、前記アクセス先通信処理装置に対するアクセス許可グループ情報としてホスト名によるアクセス許可グループ情報を格納した許可グループデータベースを参照して、アクセス先通信処理装置のアクセス許可グループにアクセス元通信処理装置が属するか否かの審査処理を実行すること
を特徴とする。

【0032】

さらに、本発明のアクセス権限管理方法の一実施態様において、前記中継サーバは、前記
アクセス先通信処理装置にネットワーク接続されたホームサーバであることを特徴とする 20

【0033】

さらに、本発明のアクセス権限管理方法の一実施態様において、前記アクセス権限管理方法において、前記中継サーバは、さらに、前記アクセス先通信処理装置に対応するドメイン名またはホスト名に対応するアドレスの更新処理を実行するステップを有し、前記アクセス先通信処理装置の有する属性証明書の検証の成立を条件として前記更新処理を実行すること
を特徴とする。

【0034】

さらに、本発明のアクセス権限管理方法の一実施態様において、前記中継サーバは、アクセス元通信処理装置との相互認証を実行し、相互認証の成立を条件として、前記アクセス元通信処理装置から提示されるグループ属性証明書の検証および審査を実行すること
を特徴とする。 30

【0035】

さらに、本発明のアクセス権限管理方法の一実施態様において、前記グループ属性証明書は、グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、前記中継サーバは、前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書の検証を併せて実行すること
を特徴とする。

【0036】

さらに、本発明の第4の側面は、
通信ネットワークを介した通信処理装置間の通信におけるアクセス権限管理処理を実行せしめるコンピュータ・プログラムであって、
アクセス元通信処理装置から、アクセス先通信処理装置のホスト名を受信するとともに、特定通信処理装置の集合からなるグループに対応して設定されるグループ識別情報を格納し発行者電子署名を有するグループ属性証明書を受信するステップ、
該グループ属性証明書の検証処理、および、アクセス先通信処理装置のアクセス許可グループにアクセス元通信処理装置が属するか否かの審査処理を実行するステップ、
該検証および審査が成立したことを条件として、名前解決サーバを適用した名前解決処理により、アクセス先通信処理装置のアドレスを取得し、前記アクセス元通信処理装置に対する通知処理を実行するステップ、 40
50

を有することを特徴とするコンピュータ・プログラムにある。

【0037】

【作用】

本発明の構成によれば、通信ネットワークを介した通信処理装置間の通信において、アクセス先の許容するアクセス元であるか否かをホームサーバ等の中継サーバにおいて判定して、アクセス先の許容するアクセス元である場合にのみ、名前解決処理を実行して、アクセス先のアドレス情報をアクセス元に通知する構成としたので、アクセス先の許容したアクセス元からのアクセスのみを実行する構成が実現される。

【0038】

さらに、本発明の構成によれば、通信ネットワークを介した通信処理装置間の通信において、ホームサーバ等の中継サーバが、アクセス元の属性証明書の検証、審査を実行して、アクセス元がアクセス先の許容メンバーであるか否かの判定処理を実行し、アクセス先の許容するアクセス元である場合にのみ、名前解決処理を実行して、アクセス先のアドレス情報をアクセス元に通知する構成としたので、属性証明書に基づく確実な審査によるアクセス制限を実行することが可能となる。

【0039】

さらに、本発明の構成によれば、アクセス元のドメイン名属性証明書、ホスト名属性証明書等、属性情報としてドメイン名、ホスト名を記述したグループ属性証明書を適用する構成としたので、特定ドメインに属する機器、あるいは特定ホスト名の機器に限定したアクセス制限を実行することが可能となる。

【0040】

さらに、本発明の構成によれば、アクセス元のドメイン名属性証明書、ホスト名属性証明書等、属性情報としてドメイン名、ホスト名を記述したグループ属性証明書を適用する構成とするとともに、ドメイン名、ホスト名に対応するアドレスの更新を実行する構成としたので、旧アドレスを適用したアクセスの排除が可能となる。

【0041】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【0042】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【0043】

【発明の実施の形態】

以下、本発明について図面を参照して詳細に説明する。なお、以下、下記に示す項目順に説明する。

- (1) アクセス権限管理システム構成概要
- (2) ユーザデバイス構成
- (3) アクセス制限処理
 - (3-1) アクセス制限処理概要
 - (3-2) ドメイン登録および属性証明書発行処理
 - (3-3) アクセス許可情報の登録および削除処理
 - (3-4) アクセス許可判定処理
 - (3-5) アドレス更新処理
- (4) 各エンティティの構成

【0044】

〔(1) アクセス権管理システム概要〕

本発明のアクセス権管理システムは、図1に示すように、公開鍵証明書(PKC: Public Key certificate) 121に基づく公開鍵基盤(PKI: Public Key infrastructure) 101、属性証明書(AC: Attribute certificate) 122に基づく権限管理基盤(PMI: Privilege management infrastructure) 102を基本インフラとし、これらのインフラの下で、耐タンパ性のセキュリティチップ(あるいはセキュリティモジュール)を持つ通信処理装置としてのユーザデバイス131~133、およびユーザデバイス141~143がネットワークを介した通信を実行する。

10

【0045】

ユーザデバイス131~133は、例えばホームサーバ等の中継サーバ130を介してネットワーク110を介した通信を実行し、ユーザデバイス141~143は、中継サーバ140を介してネットワーク110を介した通信を実行する。

【0046】

ユーザデバイス131~133とホームサーバ等の中継サーバ130とは、サブネットワークを構成し、例えばイーサネット等の有線あるいは無線LAN、その他の通信ネットワークにより接続され、中継サーバ130は、以下、詳細に説明するグループ属性証明書等、属性証明書122に基づいて、自己の管理領域内のユーザデバイス131~133に対するアクセス要求に関するアクセス権限の判定処理を実行し、アクセス権限があると判定されたアクセス要求のみに対して、DNS(Domain Name System)としての名前解決サーバ135によるホスト名からアドレスへの変換処理を実行し、名前解決により取得したアクセス先のアドレスデータをアクセス要求元に対して通知する。中継サーバ140も、同様にグループ属性証明書等の属性証明書122に基づいて、自己の管理領域内のユーザデバイス141~143に対するアクセス要求のアクセス権限を判定し、同様の処理を実行する。

20

【0047】

ユーザデバイス131~133, 141~143は、ネットワーク110を介したユーザデバイス間における通信処理が実行可能な端末であり、具体的には、PC、ゲーム端末、DVD、CD等の再生装置、携帯通信端末、PDA、メモリカード等によって構成され、耐タンパ構成のセキュリティチップを搭載している。ユーザデバイスの詳細については後述する。

30

【0048】

なお、図1では、ユーザデバイス相互間の通信制御構成を示してあるが、ユーザデバイスが、サービスプロバイダから音楽、画像、プログラム等の各種コンテンツ提供サービス、その他の情報利用サービス、決済サービス等の各種サービスの提供を受領する場合にも、同様の属性証明書を適用したアクセス権限の判定、および判定に基づく名前解決処理の実行プロセスが可能であり、本発明のアクセス権管理システムは、ユーザデバイス間のアクセス制御のみならず、サービスプロバイダとユーザデバイス間など、さまざまなエンティティ間の通信におけるアクセス制御に適用可能である。

40

【0049】

(公開鍵証明書: PKC)

次に、公開鍵基盤について説明する。公開鍵基盤(PKI: Public Key infrastructure) 101は、公開鍵証明書(PKC: Public Key certificate)を適用して通信エンティティ間の認証処理、あるいは転送データの暗号処理等を実行可能とした基盤(インフラ)である。(公開鍵証明書(PKC))について図2、図3、図4を用いて説明する。公開鍵証明書は、認証局(CA: Certification Authority)が発行する証明書であり、ユーザ、各エンティティが自己のID、公開鍵等を認証局に提出することにより、認証局側が認証局のIDや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

50

【0050】

なお、認証局（CA）の事務代理機関として、登録局（RA:Registration Authority）を設け、登録局（RA）において、公開鍵証明書（PKC）の発行申請受理、申請者の審査、管理を行なう構成が一般的となっている。

【0051】

公開鍵証明書のフォーマット例を図2～図4に示す。これは、公開鍵証明書フォーマットITU-T X.509に準拠した例である。

【0052】

バージョン（version）は、証明書フォーマットのバージョンを示す。

シリアルナンバ（Serial Number）は、公開鍵証明書発行局（CA）によって設定される公開鍵証明書のシリアルナンバである。

シグネチャ（Signature）は、証明書の署名アルゴリズムである。なお、署名アルゴリズムとしては、楕円曲線暗号およびRSAがあり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、RSAが適用されている場合には鍵長が記録される。

発行者（issuer）は、公開鍵証明書の発行者、すなわち公開鍵証明書発行局（IA）の名称が識別可能な形式（Distinguished Name）で記録されるフィールドである。

有効期限（validity）は、証明書の有効期限である開始日時、終了日時が記録される。

サブジェクト公開鍵情報（subject Public Key Info）は、証明書所有者の公開鍵情報として鍵のアルゴリズム、鍵が格納される。

【0053】

証明局鍵識別子（authority Key Identifier-key Identifier、authority Cert Issuer、authority Cert Serial Number）は、署名検証に用いる証明書発行者の鍵を識別する情報であり、鍵識別子、機関証明書発行者の名称、機関証明書シリアル番号を格納する。

サブジェクト鍵識別子（subject key Identifier）は、複数の鍵を公開鍵証明書において証明する場合に各鍵を識別するための識別子を格納する。

鍵使用目的（key usage）は、鍵の使用目的を指定するフィールドであり、（0）デジタル署名用、（1）否認防止用、（2）鍵の暗号化用、（3）メッセージの暗号化用、（4）共通鍵配送用、（5）認証の署名確認用、（6）失効リストの署名確認用の各使用目的が設定される。

秘密鍵有効期限（private Key Usage Period）は、証明書に格納した公開鍵に対応する秘密鍵の有効期限を記録する。

認証局ポリシー（certificate Policies）は、公開鍵証明書発行者の証明書発行ポリシーを記録する。例えばISO/IEC 9384-1に準拠したポリシーID、認証基準である。

ポリシー・マッピング（policy Mapping）は、認証パス中のポリシー関係の制限に関する情報を格納するフィールドであり、認証局（CA）証明書にのみ必要となる。

サブジェクト別名（subject Alt Name）は、証明書所有者の別名を記録するフィールドである。

発行者別名（issuer Alt Name）は、証明書発行者の別名を記録するフィールドである。

サブジェクト・ディレクトリ・アトリビュート（subject Directory Attribute）は、証明書所有者のために必要とされるディレクトリの属性を記録するフィールドである。

基本制約（basic Constraint）は、証明対象の公開鍵が認証局（CA）

の署名用か、証明書所有者のものを区別するためのフィールドである。

許容サブツリー制約名 (name Constraints permitted Subtrees) は、発行者が発行する証明書の名前の制限情報を格納するフィールドである。

制約ポリシー (policy Constraints) は、認証パス中のポリシーの關係の制限情報を格納するフィールドである。

CRL参照ポイント (Certificate Revocation List Distribution Points) は、証明書所有者が証明書を利用する際に、証明書が失効していないか、どうかを確認するための失効リストの参照ポイントを記述するフィールドである。

10

署名アルゴリズム (Signature Algorithm) は、証明書の署名付けに用いるアルゴリズムを格納するフィールドである。

署名は、公開鍵証明書発行者の署名フィールドである。電子署名は、証明書全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して発行者の秘密鍵を用いて生成したデータである。署名付けやハッシュをとるだけでは改竄は可能であるが、検出できれば実質的に改竄できないことと同様の効果がある。

【0054】

認証局は、図2～図4に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための失効リスト (Revocation List) の作成、管理、配布 (これをリボケーション: Revocationと呼ぶ) を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

20

【0055】

一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。

【0056】

(属性証明書: AC)

権限管理基盤 (PMI: Privileged management Infrastructure) 102は、属性証明書 (AC: Attribute certificate) 122を適用した権限確認処理を実行可能とする基盤 (インフラ) である。属性証明書の1形態としてのグループ属性証明書 (グループAC) について図5乃至図7を参照して説明する。本発明におけるシステムで適用する属性証明書の機能は、アクセス権限、サービス利用権限の確認機能であり、属性証明書には、例えば特定の通信処理装置としてのユーザデバイス (エンドエンティティ) に対するアクセス許可情報として適用可能な所有者の属性情報が記述される。

30

【0057】

属性証明書は、基本的には属性認証局/属性証明書発行局 (AA: Attribute Authority) が発行する証明書であり、証明書発行対象の属性情報を格納し、属性認証局/属性証明書発行局側がIDや有効期限等の情報を付加し、さらに属性認証局/属性証明書発行局の秘密鍵による署名を付加して作成される証明書である。ただし、以下において説明するグループ属性証明書は、必ずしも属性認証局/属性証明書発行局 (AA: Attribute Authority) が発行機関として限定されるものではなく、サービスプロバイダ、ホームサーバ等の中継サーバ、ユーザデバイスにおける発行処理が可能である。

40

【0058】

なお、属性認証局/属性証明書発行局 (AA) の事務代理機関として、属性証明書登録局 (ARA: Attribute Registration Authority) を設け、属性証明書登録局 (ARA) において、属性証明書 (AC) の発行申請受理、申請者の審査、管理を行なう構成により、処理負荷の分散が可能である。

50

【0059】

本発明の構成において適用されるグループ属性証明書（グループAC）は、複数の対象、例えば複数のユーザ、あるいは複数のユーザ機器を1つの同一属性集合としたグループとして設定し、設定したグループを単位として、グループの構成機器または構成ユーザに対して発行される属性証明書である。グループ属性証明書は、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名の付加された証明書である。

【0060】

例えば複数人が所属している会社、組織、学校といった属性、あるいは家族といったグループに属する各ユーザまたはユーザ機器に対して発行される。あるいは、1つのサービスプロバイダの提供するサービスを受領する複数のユーザ単位といったグループのメンバー（ユーザ、ユーザ機器）に対して発行される。また、例えばドメイン名、ホスト名によるグループ定義が適用可能である。グループについては、様々な設定が可能であり、具体例については、後述する。

【0061】

属性証明書の基本フォーマットはITU-T X.509で規定されており、IETF PKIX WGでProfileを策定している。公開鍵証明書とは異なり所有者の公開鍵を含まない。しかし属性証明書認証局（Attribute Certificate Authority）の署名がついているため、改竄されていないかどうかの判定はこの署名を検証することで行える、という点は公開鍵証明書と同様である。

【0062】

なお、本発明において適用するグループ属性証明書は、属性証明書の基本フォーマットに準拠したものとして構成可能である。ただし、ITU-T X.509で規定されたフォーマットに従うことが必須ではなく、独自フォーマットとした属性証明書構成としてもよい。

【0063】

本発明の構成においては、属性証明書（AC）の発行管理を行なう属性証明書認証局（AA: Attribute Certificate Authority）、および属性証明書登録局（ARA）の機能を、サービスプロバイダ、ホームサーバ、あるいはユーザデバイスが兼務することが可能である。すなわち、サービスプロバイダ、ホームサーバあるいはユーザデバイス自身が、属性証明書認証局（AA）、属性証明書登録局（ARA）の各機能を果たす構成が可能である。

【0064】

属性証明書は基本的に公開鍵証明書と関連づけて利用する。すなわち属性証明書所有者の本人性自体は公開鍵証明書で確認し、その上で所有者にいかなる権限が与えられているかを属性証明書によって確認する。例えば特定のユーザデバイス（エンドエンティティ）に対するアクセス権限があるか否かを、そのユーザデバイス（エンドエンティティ）を管轄する中継サーバとしてのホームサーバがアクセス要求元の属性証明書を検証して確認する。属性証明書の検証にあたっては、当該証明書の署名検証を行った後、その属性証明書に関連づけられている公開鍵証明書の検証も行なう。

【0065】

なお、その際、原則的には証明書連鎖をたどって最上位の公開鍵証明書まで順に検証を実施することが好ましい。複数の認証局（CA）が存在し、階層構成をなす認証局構成では、下位の認証局自身の公開鍵証明書は、その公開鍵証明書を発行する上位認証局によって署名されている。すなわち、下層の公開鍵証明書発行局（CA-Low）に対して上位の公開鍵証明書発行局（CA-High）が公開鍵証明書を発行するという連鎖的な公開鍵証明書発行構成をとる。公開鍵証明書の連鎖検証とは、下位から上位へ証明書連鎖をたどって最上位の公開鍵証明書までの連鎖情報を取得して、最上位（ルートCA）までの公開鍵証明書の署名検証を行なうことを意味する。

【0066】

属性証明書の有効期間を短期間とすることにより、失効処理を行わないことも可能である。この場合、証明書の失効手続きや失効情報の参照手順等を省くことができ、システムが簡易となる長所がある。ただし証明書の不正利用に対しては失効以外の何らかの対策が必要となるため、十分に注意しなければならない。

【0067】

図5を参照してグループ属性証明書の構成について説明する。

証明書のバージョン番号は、証明書フォーマットのバージョンを示す。

AC保持者の公開鍵証明書情報、これは属性証明書(AC)の発行者に対応する公開鍵証明書(PKC)に関する情報であり、PKC発行者名、PKCシリアル番号、PKC発行者固有識別子等の情報であり、対応公開鍵証明書を関連づけるリンクデータとしての機能を持つ。 10

属性証明書の発行者の名前は、属性証明書の発行者、すなわち属性証明書認証局(AA)の名称が識別可能な形式(Distinguished Name)で記録されるフィールドである。

署名アルゴリズム識別子は、属性証明書の署名アルゴリズム識別子を記録するフィールドである。

証明書の有効期限は、証明書の有効期限である開始日時、終了日時が記録される。

属性情報フィールドには、グループ属性証明書のグループを識別するグループ識別情報としてグループID、ドメイン名、ホスト名など、グループを特定する属性情報が格納される。 20

【0068】

なお、属性情報フィールドには、グループ識別情報(グループID、ドメイン名、ホスト名など、)以外にも、様々な情報が格納可能であり、例えば、アクセス権限期間情報、その他アクセス権限に関する詳細情報を格納することが可能である。

【0069】

属性証明書には、さらに、署名アルゴリズムが記録され、属性証明書発行者、例えば属性証明書認証局(AA)によって署名が施される。発行者がサービスプロバイダ、ホームサーバ、あるいはユーザデバイスである場合は、各発行者の署名がなされる。電子署名は、属性証明書全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して属性証明書発行者の秘密鍵を用いて生成したデータである。 30

【0070】

グループ属性証明書は、グループ属性証明書を発行するエンティティ、例えば属性証明書認証局(AA:Attribute Certificate Authority)、属性証明書認証局(AA)の事務代行を行なう属性証明書登録局(ARA:Attribute Registration Authority)、あるいはサービスプロバイダ、ホームサーバ、ユーザデバイスにおいて管理される発行ポリシーに基づいて発行処理がなされる。

【0071】

グループ属性証明書を発行するエンティティは、発行ポリシーテーブルを有し、自己が発行したグループ属性証明書のグループ識別情報(グループID、ドメイン名、ホスト名など)、グループ情報、発行基準等の発行ポリシーとを対応付けたデータを有する。また、グループ属性証明書の新規発行、追加発行、更新処理等に際し、グループ属性証明書の発行ポリシーテーブルに基づいて、審査が実行され、ポリシーを満足する場合に限り、発行、更新等の手続きがなされる。 40

【0072】

図6にグループ属性証明書(グループAC)の発行者、所有者、検証者、属性情報の構成例を示す。

【0073】

(a)は単一機器によるグループであり、発行者:鈴木家ホームサーバ(HS)、所有者:鈴木一郎の携帯電話、グループ:鈴木一郎として定義されたグループのグループ属性証 50

明書（グループAC）である。（b）は複数機器によるグループであり、発行者：鈴木家ホームサーバ（HS）、所有者：鈴木家のホームサーバ（HS）、ビデオカメラ、冷蔵庫の各機器であり、グループ：鈴木一郎所有機器、として定義されたグループのグループ属性証明書（グループAC）である。

【0074】

（c）は複数機器によるグループであり、発行者：メーカーX、所有者：ビデオデッキの各機器であり、グループ：メーカーX製造のビデオデッキ、として定義されたグループのグループ属性証明書（グループAC）である。（d）は複数ユーザによるグループであり、発行者：グループ属性証明書認証局（AA）、所有者：鈴木家のメンバーであり、グループ：鈴木家、として定義されたグループのグループ属性証明書（グループAC）である 10

。

【0075】

（e）はドメイン名によるグループ定義のされたドメイン名属性証明書であり、例えば発行者：ドメイン名グループ属性証明書認証局（AA）、所有者：鈴木家HS、テレビ、カメラであり、グループドメイン：suzuki.abc.net、として定義されたグループのグループ属性証明書（グループAC）である。同じドメインに属する通信処理装置は、同じグループドメインを属性情報として有するドメイン名グループ属性証明書を保有することになる。

【0076】

（f）はホスト名によるグループ定義のされたホスト名属性証明書であり、例えば発行者 20：ホスト名グループ属性証明書認証局（AA）、所有者：鈴木家テレビであり、グループホスト名：tv1.suzuki.abc.net、として定義されたグループのグループ属性証明書（グループAC）である。

【0077】

上述のような、様々な定義のグループの所属機器またはユーザを対象としてグループ属性証明書が発行される場合、発行されたグループ属性証明書は、ユーザの所有する機器内に格納される。ユーザデバイスの詳細については後述する。

【0078】

ユーザデバイスに対して発行されたグループ属性証明書に基づいてアクセス権限確認を実行する検証者は、例えば、図1に示すホームサーバ等の中継サーバであり、中継サーバの 30管理領域内のユーザデバイス（通信処理装置）に対するアクセスの要求機器からグループ属性証明書を受領して、受領したグループ属性証明書の検証および審査を実行して、アクセス権限が確認されたことを条件として名前解決サーバに対してホスト名からアドレスへの変換処理を依頼し、取得アドレスをアクセス要求元に通知することで、受領アドレスを適用した通信が可能となる。属性証明書の検証、審査の結果、アクセス権限が認められない場合は、名前解決サーバによるホスト名からアドレスへの変換が実行されず、アクセス要求元はアクセス要求先のアドレスを得ることができず、通信処理は実行されない。

【0079】

図6を参照して説明した様々なグループ定義に基づくグループ属性証明書中の（e）ドメイン名グループ、（f）ホスト名グループの各グループ定義に基づく属性証明書構成例を 40図7に示す。（e）ドメイン名グループ属性証明書は、属性情報フィールドにドメイン名が記述され、特定のドメインが識別される。一方、（f）ホスト名グループ属性証明書は、属性情報フィールドにホスト名が記述され、特定のホストが識別可能となる。

【0080】

図8を参照して、ドメイン名グループ属性証明書の発行体系について説明する。ドメイン名グループ属性証明書は、原則的に所属ドメインの上位のドメイン名属性証明書登録局（ARA:Attribute Registration Authority）を通じてドメイン名属性証明書認証局（AA）から発行される。なお、ドメイン名AAは単一であるとは限らず、複数存在してもよい。また、ドメインの公共性を考慮して運営主体は独立した事業体であることが望ましい。

【0081】

図8には、ドメインとして上位から、abc.netドメイン151、home1.abc.netドメイン152、sub.home1.abc.netドメイン153の3ドメイン領域が示されている。上位ドメインは、下位ドメインを含む構成である。

【0082】

abc.netドメイン151のサービスプロバイダ155に対するドメイン名グループ属性証明書は、上位のドメイン名属性証明書登録局（ARA）であるセカンドレベルドメイン割当機関154が、サービスプロバイダ155の要求に基づいて、発行ポリシーに基づく発行手続きを行ない、ポリシーに従っていることを条件として、ドメイン名属性証明書認証局（AA）150の発行したドメイン名グループ属性証明書161をサービスプロバイダ155に送付する。 10

【0083】

abc.netドメイン151の下位ドメインであるhome1.abc.netドメイン152のホームサーバ156、または、エンドエンティティ（ユーザデバイス）であるEE A158に対するドメイン名グループ属性証明書は、上位のドメイン名属性証明書登録局（ARA）であるサービスプロバイダ155が、ホームサーバ156、EE A158の要求に基づいて、発行ポリシーに基づく発行手続きを行ない、ポリシーに従っていることを条件として、ドメイン名属性証明書認証局（AA）150の発行したドメイン名グループ属性証明書162、163をホームサーバ156、EE A158に送付する。 20

【0084】

home1.abc.netドメイン152の下位ドメインであるsub.home1.abc.netドメイン153のホームサーバ157、または、エンドエンティティ（ユーザデバイス）であるEE P159、EE Q160に対するドメイン名グループ属性証明書は、上位のドメイン名属性証明書登録局（ARA）であるホームサーバ156が、ホームサーバ157、EE P159、EE Q160の要求に基づいて、発行ポリシーに基づく発行手続きを行ない、ポリシーに従っていることを条件として、ドメイン名属性証明書認証局（AA）150から発行されたドメイン名グループ属性証明書164～166をホームサーバ157、EE P159、EE Q160に送付する。

【0085】

このように、ドメイン名グループ属性証明書は、上位のドメイン名属性証明書登録局（ARA）が、下位のドメインに属するメンバー（機器）に対して発行ポリシーに従って発行する処理を実行する。 30

【0086】

次に、図9を参照してホスト名グループ属性証明書の発行体系について説明する。ホスト名グループ属性証明書は、原則的に所属ドメインのホスト名属性証明書登録局（ARA：Attribute Registration Authority）を通じてドメイン名属性証明書認証局（AA）から発行される。なお、ホスト名AAはサービスプロバイダが運営してもよい。

【0087】

図9には、図8と同様、ドメインとして上位から、abc.netドメイン、home1.abc.netドメイン、sub.home1.abc.netドメインの3ドメインのそれぞれに属するエンティティが記載され、abc.netドメインには、サービスプロバイダ155が所属し、home1.abc.netドメインには、ホームサーバ156、およびエンドエンティティ（ユーザデバイス）であるEE A158が所属し、sub.home1.abc.netドメインには、ホームサーバ157、およびエンドエンティティ（ユーザデバイス）であるEE P159、EE Q160が所属している。 40

【0088】

home1.abc.netドメインのホームサーバ156、または、エンドエンティティ（ユーザデバイス）であるEE A158に対するホスト名グループ属性証明書は、所属ドメインに対応するホスト名属性証明書登録局（ARA）であるホームサーバ156が 50

、発行ポリシーに基づく発行手続きを行ない、ポリシーに従っていることを条件として、ホスト名属性証明書認証局（AA）171から発行されたホスト名グループ属性証明書173、174をホームサーバ156、EE A158に送付する。

【0089】

home1.abc.netドメイン152の下位ドメインであるsub.home1.abc.netドメイン153のホームサーバ157、または、エンドエンティティ（ユーザデバイス）であるEE P159、EE Q160に対するホスト名グループ属性証明書は、所属ドメインに対応するホスト名属性証明書登録局（ARA）であるホームサーバ157が、発行ポリシーに基づく発行手続きを行ない、ポリシーに従っていることを条件として、ホスト名属性証明書認証局（AA）172から発行されたドメイン名グループ属性証明書175～177をホームサーバ157、EE P159、EE Q160に送付する。 10

【0090】

このように、ホスト名グループ属性証明書は、対応するドメイン内のドメイン名属性証明書登録局（ARA）が、自己のドメインに属するメンバーに対して発行ポリシーに従って発行する処理を実行する。

【0091】

発行された属性証明書は、サービスプロバイダの機器内のセキュリティモジュール（SM：Security Module）、あるいはホームサーバ等の中継サーバ、あるいはユーザデバイスのセキュリティチップ（SC：Security Chip）での署名検証による検証の後、格納される。ホームサーバ等の中継サーバ、ユーザデバイスのセキュリティチップ、サービスプロバイダの機器内のセキュリティモジュールは、外部からのデータ読み出しの制限された耐タンパ構成を持つことが好ましい。 20

【0092】

図10にアクセス権限管理システムに参加する各エンティティの信頼関係構成を説明するトラストモデルを示す。

【0093】

システムホルダ（SH：System Holder）180は、本発明のアクセス権限管理システム全体の統括的管理を行なう主体、すなわちシステム運用主体であり、システムに参加する各エンティティのセキュリティチップ（SC）、セキュリティモジュール（SM）の正当性を保証するとともに、公開鍵証明書（PKC）の発行責任を持つ。システムホルダ（SH）180は、最上位認証局としてのルートCA（Root CA）181、階層構成の複数の認証局（CA）182、および公開鍵証明書発行事務局としての登録局（RA）183を有する。 30

【0094】

システムホルダ（SH：System Holder）180は、属性証明書認証局（AA）184、属性証明書登録局（ARA）185、サービスプロバイダ187、ドメイン領域190に属する中継サーバとしてのホームサーバ192、およびユーザデバイスとしてのエンドエンティティ（EE）191の各エンティティに対応する公開鍵証明書（PKC）を発行し、各エンティティは、必要とするエンティティの公開鍵証明書を格納する。 40

【0095】

また、グループ属性証明書（グループAC）は、サービスプロバイダ187、中継サーバとしてのホームサーバ192、およびユーザデバイスとしてのエンドエンティティ（EE）191の各エンティティ等からの要求にしたがって、それぞれのエンティティに対応して設定される属性証明書登録局（ARA）185においてポリシー（発行条件等）に従って属性証明書発行審査を行ない、発行可と判定された場合に属性証明書認証局（AA）184に対して、属性証明書登録局（ARA）185から発行依頼を転送する。

【0096】

属性証明書認証局（AA）184は、グループ属性証明書発行依頼に基づいて、先に説明したドメイン名、あるいはホスト名、グループIDなどの情報をグループ識別情報として 50

属性情報領域に格納し、属性証明書認証局（AA）184の秘密鍵による署名を付加したグループ属性証明書（図5参照）を発行要求者に対して発行する。

【0097】

なお、前述したように、これら属性証明書認証局（AA）184、および属性証明書登録局（ARA）185は、サービスプロバイダ、ホームサーバ、あるいはユーザデバイスがその機能を実行する構成とすることも可能である。

【0098】

〔（2）セキュリティチップ構成〕

次に通信ネットワークを介した通信を実行する通信処理装置としてのユーザデバイスあるいは中継サーバとしてのホームサーバ、およびサービスプロバイダ等に構成されるセキュリティチップ（またはモジュール）の構成について説明する。なお、ユーザデバイスは、通信実行機器としてのエンドエンティティ（EE）であり、他の通信処理装置との通信を実行するインタフェースを持つ例えばPC、ホームサーバ、PDA等の携帯端末、ICカード等、各種データ処理装置である。

【0099】

通信処理装置としてのユーザデバイス（エンドエンティティ）あるいは中継サーバとしてのホームサーバ、およびサービスプロバイダなどに構成されるセキュリティチップ（またはモジュール）の構成例について、図11を参照して説明する。

【0100】

図11に示すように、ユーザデバイス（エンドエンティティ）あるいは中継サーバとしてのホームサーバ、およびサービスプロバイダなどのデバイス200には、セキュリティチップ210が、デバイス側制御部221に対して、相互にデータ転送可能な構成として内蔵される。

【0101】

セキュリティチップ210は、プログラム実行機能、演算処理機能を持つCPU（Central Processing Unit）201を有し、データ通信用のインタフェース機能を持つ通信インタフェース202、CPU201によって実行される各種プログラム、例えば暗号処理プログラムなどを記憶するROM（Read Only Memory）203、実行プログラムのロード領域、また、各プログラム処理におけるワーク領域として機能するRAM（Random Access Memory）204、外部機器との認証処理、電子署名の生成、検証処理、格納データの暗号化、復号化処理等の暗号処理を実行する暗号処理部205、各種鍵データを含むデバイスの固有情報を格納した例えばEEPROM（Electrically Erasable Programmable ROM）によって構成されるメモリ部206を有する。

【0102】

デバイス200は、暗号化コンテンツあるいはサービス情報等を格納する領域としてのEEPROM、ハードディスク等によって構成される外部メモリ部222を有する。外部メモリ部222は、公開鍵証明書、グループ属性証明書の格納領域としても利用可能である。

。

【0103】

セキュリティチップを搭載したユーザデバイスが、外部エンティティ、例えばネットワーク接続された他のユーザデバイス、中継サーバとしてのホームサーバ、あるいはサービスプロバイダと接続して通信処理を実行する場合には、ネットワークインタフェース232を介した接続を実行する。ただし、ネットワークインタフェース232を持たないユーザデバイスは、接続機器インタフェース231を介して通信機能を持つエンドエンティティ（EE）に接続して、エンドエンティティのネットワークインタフェース232を介した通信を実行する。

【0104】

図11に示すセキュリティチップを持つユーザデバイスあるいは中継サーバとしてのホームサーバ、およびサービスプロバイダ等が接続し、エンティティ間でデータ転送を実行す

10

20

30

40

50

る場合には、必要に応じて相互認証が行われる。これらの処理の詳細については、後段で詳述する。

【0105】

ユーザデバイスのセキュリティチップの格納データ例を図12に示す。これらの多くは、不揮発性メモリの一形態であるフラッシュメモリ等のEEPROM (Electrically Erasable Programmable ROM) によって構成されるメモリ部206に格納されるが、公開鍵証明書、グループ属性証明書は、セキュリティチップ内のメモリに格納しても、外部メモリに格納してもよい。

【0106】

各データについて説明する。

10

公開鍵証明書 (PKC) : 公開鍵証明書は、第三者に対して正当な公開鍵であることを示す証明書で、証明書には配布したい公開鍵を含み、信頼のおける認証局により電子署名がなされている。ユーザデバイスには、前述した階層構成の最上位認証局 (ルートCA) の公開鍵証明書、ユーザデバイスに対するサービスを提供するサービスプロバイダの公開鍵証明書等、ユーザデバイスとのデータ通信を実行する際の認証、暗号化、復号処理等に適用する公開鍵を取得するために必要となる公開鍵証明書が格納される。

【0107】

グループ属性証明書 (AC) : 公開鍵証明書が証明書利用者 (所有者) の“本人性”を示すのに対し、グループ属性証明書は証明書利用者のグループを識別しグループの構成メンバーに付与された利用権限を確認するものである。利用者はグループ属性証明書を提示することにより、グループ属性証明書に記載された権利・権限に基づいて、アクセスが行えるようになる。なお、グループ属性証明書は所定の発行手続きに基づいて発行される。これらの処理の詳細は後述する。

20

【0108】

鍵データ : 鍵データとしては、セキュリティチップに対して設定される公開鍵、秘密鍵のペア、さらに、乱数生成用鍵、相互認証用鍵等が格納される。

【0109】

識別情報 : 識別情報としては、セキュリティチップ自身の識別子としてのセキュリティチップIDが格納される。さらに継続的なサービス提供を受けるサービスプロバイダ (SP) の識別子としてのサービスプロバイダID、ユーザデバイスを利用するユーザに付与されたユーザID、サービスプロバイダの提供するサービスに対応するアプリケーションを識別するアプリケーションID等が格納可能である。

30

【0110】

その他 : ユーザデバイスには、さらに、乱数生成用のシード情報、すなわち認証処理、暗号処理等の際に適用する乱数をANSI X9.17に従って生成するための情報や、様々な利用制限が付加されたサービスに関する利用情報、例えば、コンテンツ利用回数制限が付加されたコンテンツを利用した際に更新されるコンテンツ利用回数情報、あるいは決済情報等の情報、あるいは、各情報に基づいて算出されるハッシュ値が格納される。

【0111】

なお、図12に示すデータ構成例は、一例であり、この他にも必要に応じて、ユーザデバイスの受領するサービスに関連する各種の情報が格納可能である。

40

【0112】

なお、データ送受信部であるネットワークインタフェースを介して受信したグループ属性証明書の検証処理の実行、あるいは、グループ属性証明書の生成処理の実行手段としても図11に示すセキュリティチップ構成が適用される。

【0113】

〔(3) アクセス制限処理〕

(3-1) アクセス制限処理概要

次に、ドメイン名、ホスト名、団体、学校、会社、あるいは1つの家族等、様々な集合に属するユーザ、あるいは、同一メーカーの機器、同一サービスプロバイダのサービスを受領

50

するユーザ、機器等、複数のユーザまたは機器をグループとして設定し、グループに属するユーザまたは機器の各々に対して発行するグループ属性証明書に基づくアクセス制限処理の詳細について説明する。

【0114】

グループ属性証明書は、ネットワークを介した通信を実行しようとするユーザまたは機器（ユーザデバイス）が特定のグループに属することを確認可能な証明書であり、他の通信処理装置に対するアクセス要求に際して、通信相手となる通信処理装置（ユーザデバイス）を管理するホームサーバ等の中継サーバに提示する。

【0115】

図13を参照して、アクセス権管理システムの概要について説明する。図13において 10、ホームサーバ等の中継サーバ1、313は、エンドエンティティ通信処理装置としてのユーザデバイス（EE-A）311を管理端末として有し、ユーザデバイス（EE-A）311に対する通信ネットワーク355を介したアクセスの許可、不許可について、アクセス要求元から送付される属性証明書、およびアクセス許可情報を格納した許可グループデータベース314の格納情報に基づいて判定する。

【0116】

一方ホームサーバ等の中継サーバ2、323は、通信処理装置としてのユーザデバイス321を管理端末として有し、ユーザデバイス321に対する通信ネットワーク355を介したアクセスの許可、不許可について、アクセス要求元から送付される属性証明書およびアクセス許可情報を格納した許可グループデータベース324の格納情報に基づいて判定 20する。

【0117】

ユーザデバイス311とホームサーバ等の中継サーバ1、313とは、ある特定のサブネットワーク名にあり、例えばイーサネット等の有線あるいは無線LAN、その他の通信ネットワークにより接続される。

【0118】

図13の中継サーバ1、313は、アクセス要求元から提示されるグループ属性証明書に基づいて、自己の管理領域内のユーザデバイス314に対するアクセス権を判定し、アクセス権があると判定されたことを条件として、DNS（Domain Name System）としての名前解決サーバ312によるホスト名からアドレスへの変換処理を 30実行し、アドレスデータをアクセス要求元に対して通知する。中継サーバ2、323も、同様にアクセス要求元から提示されるグループ属性証明書に基づいて、自己の管理領域内のユーザデバイス324に対するアクセス要求のアクセス権を判定し、同様の処理を実行する。

【0119】

図13に示すサービスプロバイダ（SP1）331は、中継サーバ313の上位ドメイン領域に属するサービスプロバイダであり、中継サーバ313または、ユーザデバイス311に対するドメイン名属性証明書の発行手続きを実行する属性証明書登録局（ARA）として機能し、中継サーバ313または、ユーザデバイス311からの属性証明書発行要求に応じて、サービスプロバイダ（SP1）331が、発行ポリシーに基づく発行手続きを行ない、ポリシーに従っていることを条件として、ドメイン名属性証明書認証局（AA）351から発行されたドメイン名属性証明書を中継サーバ313または、ユーザデバイス311に送付する。 40

【0120】

サービスプロバイダ（SP2）341は、中継サーバ323の上位ドメイン領域に属するサービスプロバイダであり、中継サーバ323または、ユーザデバイス321に対するドメイン名属性証明書の発行手続きを実行する属性証明書登録局（ARA）として機能し、中継サーバ323または、ユーザデバイス321からの属性証明書発行要求に応じて、サービスプロバイダ（SP2）341が、発行ポリシーに基づく発行手続きを行ない、ポリシーに従っていることを条件として、ドメイン名属性証明書認証局（AA）352から発 50

行されたドメイン名属性証明書の中継サーバ323または、ユーザデバイス321に送付する。

【0121】

また、サービスプロバイダ（SP1）331、サービスプロバイダ（SP2）341も、通信ネットワーク355を介した通信処理においてそれぞれの名前解決サーバ333、343により、ホスト名からアドレスへの変換処理を実行し、アドレスデータをアクセス要求元に対して通知する処理を実行する。

【0122】

サービスプロバイダ（SP1）331の利用する名前解決サーバ333、および、中継サーバ313の利用する名前解決サーバ312の有するデータベース例を図14に示す。 10

【0123】

図14（a）は、サービスプロバイダ（SP1）331の利用する名前解決サーバ333のデータベース例であり、自己の属するドメイン[a b c . n e t]の配下のドメインに対応するドメイン名に対応するアドレス空間、および中継サーバとしてのホームサーバのIPアドレスの各データが格納された構成を持つ。

【0124】

図14（b）は、中継サーバ313の利用する名前解決サーバ312の有するデータベース例であり、自己の属するドメイン[h o m e 1 . a b c . n e t]に属する機器のホスト名に対応するIPアドレスが格納され、さらに上位ドメインの名前解決サーバ、図13の構成では名前解決サーバ333のIPアドレスデータが格納されている。 20

【0125】

サービスプロバイダ、ホームサーバ等の中継サーバは、通信ネットワークを介する通信処理において、アクセス要求元からホスト名を受信し、名前解決サーバを利用してアドレスを取得して、アドレス情報をアクセス要求元に通知し、アドレスに基づく通信を可能とする処理を実行する。

【0126】

（3-2）ドメイン登録および属性証明書発行処理

次に、ドメイン登録申請処理、およびドメイン名属性証明書の取得処理について説明する。

【0127】

まず、図15、図16を参照して1以上の通信処理装置としてのユーザデバイスを管理するホームサーバによるドメイン登録申請処理、およびドメイン名属性証明書の取得処理手順を説明する。なお、図15、図16において、

ホーム名前解決サーバ：ホームサーバの利用する名前解決サーバ、

ホームサーバ：属性証明書に基づく審査に基づいてホーム名前解決サーバを利用した名前解決を実行する中継サーバ、

サービスプロバイダ（SP）：ホームサーバに対するドメイン名付与を実行するサービスプロバイダ、

SP名前解決サーバ：サービスプロバイダ（SP）が名前解決を実行するために利用する名前解決サーバ、 40

ドメイン名ARA：ドメイン名属性証明書登録局、

ドメイン名AA：ドメイン名属性証明書認証局、

である。

【0128】

図15は、ホームサーバによるドメイン登録申請処理手順を示しており、ステップS11において、ユーザがホームサーバに対してドメイン登録開始処理コマンドを入力すると、ステップS12において、ホームサーバは、自己の属するドメインの管理サービスプロバイダに対してドメイン登録申請を送信する。

【0129】

ステップS13では、ホームサーバと、ドメイン登録申請を受領したサービスプロバイダ 50

との間で相互認証処理が実行される。相互認証は、データ送受信を実行する2つのエンティティ間で相互に相手が正しいデータ通信者であるか否かの確認のために実行される処理である。認証成立を条件として必要なデータ転送を行なう。また、相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として、その後は、セッション鍵に基づく暗号化処理を施したデータ転送を行なう構成が好ましい。相互認証方式としては、公開鍵暗号方式、共通鍵暗号方式等、各方式の適用が可能である。

【0130】

ここでは、公開鍵暗号方式の1つの認証処理方式であるハンドシェイクプロトコル(TLS1.0)について図17のシーケンス図を参照して説明する。

【0131】

図17において、エンティティA(クライアント)、エンティティB(サーバ)が、通信を実行する2エンティティであり、ここではホームサーバまたはサービスプロバイダに対応する。まず、(1)エンティティBが暗号化仕様を決定するためのネゴシエーション開始要求をハローリクエストとしてエンティティAに送信する。(2)エンティティAはハローリクエストを受信すると、利用する暗号化アルゴリズム、セッションID、プロトコルバージョンの候補をクライアントハローとして、エンティティB側に送信する。

【0132】

(3)エンティティB側は、利用を決定した暗号化アルゴリズム、セッションID、プロトコルバージョンをサーバハローとしてエンティティAに送信する。(4)エンティティBは、自己の所有するルートCAまでの公開鍵証明書(X.509v3)一式をエンティティAに送信(サーバ・サーティフィケート)する。なお、証明書連鎖をたどって最上位の公開鍵証明書まで順に検証を実施しない場合には、必ずしもルートCAまでの公開鍵証明書(X.509v3)一式を送付する必要はない。(5)エンティティBは、RSA公開鍵またはDiffie & Hellman公開鍵情報をエンティティAに送信(サーバ・キー・エクスチェンジ)する。これは証明書が利用できない場合に一時的に適用する公開鍵情報である。

【0133】

(6)次にエンティティB側は、エンティティAに対してサーティフィケート・リクエストとして、エンティティAの有する証明書を要求し、(7)エンティティBによるネゴシエーション処理の終了を知らせる(サーバハロー終了)。

【0134】

(8)サーバハロー終了を受信したエンティティAは、自己の所有するルートCAまでの公開鍵証明書(X.509v3)一式をエンティティBに送信(クライアント・サーティフィケート)する。なお、公開鍵証明書の連鎖検証を行わない場合は公開鍵証明書の一式送付は必須ではない。(9)エンティティAは、48バイト乱数をエンティティBの公開鍵で暗号化してエンティティBに送信する。エンティティB、エンティティAは、この値をもとに送受信データ検証処理のためのメッセージ認証コード:MAC(Message Authentication Code)生成用のデータ等を含むマスターシークレットを生成する。

【0135】

(10)エンティティAは、クライアント証明書の正しさを確認するため、ここまでのメッセージのダイジェストをクライアントの秘密鍵で暗号化してエンティティBに送信(クライアントサーティフィケート確認)し、(11)先に決定した暗号化アルゴリズム、鍵利用の開始を通知(チェンジ・サイファー・スペック)し、(12)認証の終了を通知する。一方、(13)エンティティB側からエンティティAに対しても、先に決定した暗号化アルゴリズム、鍵利用の開始を通知(チェンジ・サイファー・スペック)し、(14)認証の終了を通知する。

【0136】

上記処理において決定された暗号化アルゴリズムに従ってエンティティAとエンティティB間のデータ転送が実行されることになる。

【0137】

データ改竄の検証は、上述の認証処理でエンティティAとエンティティB間の合意のもとに生成されたマスターシークレットから算出されるメッセージ認証コード：MAC (Message Authentication Code) を各エンティティの送信データに付加することでメッセージの改竄検証を行なう。

【0138】

図18にメッセージ認証コード：MAC (Message Authentication Code) の生成構成を示す。データ送信側は、送信データに対して、認証処理において生成したマスターシークレットに基づいて生成されるMACシークレットを付加し、これらの全体データからハッシュ値を計算し、さらにMACシークレット、パディング、ハッシュ値に基づいてハッシュ算出を行なってメッセージ認証コード (MAC) を生成する。この生成したMACを送信データに付加して、受信側で受信データに基づいて生成したMACと受信MACとの一致が認められればデータ改竄なしと判定し、一致が認められない場合には、データの改竄があったものと判定する。

【0139】

図15に示すステップS13において、ホームサーバとサービスプロバイダ (SP) との間で、例えば上述したシーケンスに従った相互認証処理が実行され、双方が正しい通信相手であることの確認がなされると、ステップS14において、サービスプロバイダ (SP) は、事前定義ポリシーに従ったドメイン登録審査を実行し、審査不合格である場合は、エラー処理、たとえばホームサーバに対して登録処理が実行不可能である旨を通知する処理などを実行する。

【0140】

審査合格である場合は、ステップS17において、ホームサーバに対して、希望ドメイン名の要求を実行し、ステップS18において、ホームサーバが希望ドメイン名をサービスプロバイダ (SP) に送信すると、サービスプロバイダは、ドメイン名未登録確認処理を実行する。これは、ステップS20以下の処理として実行され、サービスプロバイダからサービスプロバイダの管轄するSP名前解決サーバに対して申請ドメイン名が送信されて、SP名前解決サーバがドメイン名の検索を実行し、申請ドメイン名が未登録か否かを判定する。登録されている場合は、ステップS17に戻り、再度、希望ドメイン名を要求する。

【0141】

申請ドメイン名が登録されていない場合は、ステップS22に進み、登録可能通知をサービスプロバイダ、さらに、サービスプロバイダからホームサーバに送信する。

【0142】

次に、ドメインの登録されたホームサーバが実行するドメイン名属性証明書 (ドメイン名AC) の発行要求に対する処理手順について図16を参照して説明する。

【0143】

ステップS31において、ホームサーバは、サービスプロバイダを介してドメイン名属性証明書登録局 (ARA) に対してドメイン名属性証明書 (ドメイン名AC) の発行要求を行なう。この際、ホームサーバの公開鍵証明書 (PKC) と、登録済みドメイン名を付加データとして送信する。

【0144】

ドメイン名属性証明書登録局 (ARA) は、発行要求に基づいて、ポリシーに従った審査を実行して、発行条件を満足すると判断すると、ステップS32において、ドメイン名属性証明書認証局 (AA) に対して、ホームサーバの公開鍵証明書 (PKC) と、登録済みドメイン名とともに、ドメイン名属性証明書発行要求を行なう。

【0145】

ドメイン名属性証明書認証局 (AA) は、ステップS33において、ホームサーバの公開鍵証明書 (PKC) と、登録済みドメイン名に基づいて、ドメイン名属性証明書を生成して、ドメイン名属性証明書登録局 (ARA) に送信する。ここで生成するドメイン名属性

証明書は、先に、図 7 (a) を参照して説明した構成を持ち、属性情報フィールドにドメイン名が格納され、ドメイン名属性証明書認証局 (AA) の秘密鍵による署名がなされたものである。

【0146】

ドメイン名属性証明書登録局 (ARA) は、受信したドメイン名属性証明書をサービスプロバイダに送信し、サービスプロバイダは、ステップ S 35 において、ホームサーバのドメイン名に対応するアドレス空間の割り当てを実行して、ステップ S 36 において、決定したドメイン名に対応するアドレス空間と、ドメイン名属性証明書 (AC) をホームサーバに送信し、一方、SP 名前解決サーバに対しても、決定したドメイン名に対応するアドレス空間と、ドメイン名属性証明書 (AC) のコピーを送信する。SP 名前解決サーバは、ドメイン名に対応するアドレス空間をデータベース (図 14 (a) 参照) に登録する。 10

【0147】

ドメイン名に対応するアドレス空間と、ドメイン名属性証明書 (AC) を受信したホームサーバは、ホームサーバの利用するホーム名前解決サーバに対して決定したドメイン名に対応するアドレス空間と、ドメイン名属性証明書 (AC) のコピーを送信する。ホーム名前解決サーバは、ドメイン名に対応するアドレス空間をデータベース (図 14 (b) 参照) に登録する。

【0148】

なお、上記処理において、ドメイン名属性証明書 (AC) を受領したホームサーバは、その署名を検証してドメイン名属性証明書 (AC) の改竄がないことを確認した後、自己のメモリに格納し、またコピーを生成する。 20

【0149】

属性証明書の生成時に属性証明書認証局 (AA) が実行する電子署名の生成、および、属性証明書の格納時にホームサーバが実行する電子署名の検証処理について、図 19、図 20 を参照して説明する。

【0150】

署名は、データ改竄の検証を可能とするために付加されるものである。前述の MAC 値を用いることも可能であり、公開鍵暗号方式を用いた電子署名を適用することも可能である。

【0151】

まず、公開鍵暗号方式を用いた電子署名の生成方法について、図 19 を用いて説明する。図 19 に示す処理は、EC-D SA (Elliptic Curve Digital Signature Algorithm)、IEEE P1363/D3) を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号 (Elliptic Curve Cryptosystem (以下、ECC と呼ぶ)) を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えば RSA 暗号 (Rivest, Shamir, Adleman) など (ANSI X9.31) を用いることも可能である。 30

【0152】

図 19 の各ステップについて説明する。ステップ S1 において、p を標数、a、b を楕円曲線の係数 (楕円曲線: $y^2 = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0 \pmod{p}$)、G を楕円曲線上のベースポイント、r を G の位数、Ks を秘密鍵 ($0 < Ks < r$) とする。ステップ S2 において、メッセージ M のハッシュ値を計算し、 $f = \text{Hash}(M)$ とする。 40

【0153】

ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値 (出力) から入力を予測することが難しく、ハッシュ関数に入力されたデータの 1 ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である。 50

る特徴を有する。ハッシュ関数としては、MD4、MD5、SHA-1などが用いられる場合もあるし、DES-CBCが用いられる場合もある。この場合は、最終出力値となるMAC（チェック値：ICVに相当する）がハッシュ値となる。

【0154】

続けて、ステップS3で、乱数 u ($0 < u < r$) を生成し、ステップS4でベースポイントを u 倍した座標 $V(X_v, Y_v)$ を計算する。なお、楕円曲線上の加算、2倍算は次のように定義されている。

【0155】

【数1】

$P = (X_a, Y_a)$, $Q = (X_b, Y_b)$, $R = (X_c, Y_c) = P + Q$ とすると、10
 $P \neq Q$ の時（加算）、

$$X_c = \lambda^2 - X_a - X_b$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

$$\lambda = (Y_b - Y_a) / (X_b - X_a)$$

$P = Q$ の時（2倍算）、

$$X_c = \lambda^2 - 2X_a$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

$$\lambda = (3(X_a)^2 + a) / (2Y_a)$$

【0156】

これらを用いて点 G の u 倍を計算する（速度は遅いが、最もわかりやすい演算方法として20
 次のように行う。 G 、 $2 \times G$ 、 $4 \times G$ ・・・を計算し、 u を2進数展開して1が立っているところに対応する $2^i \times G$ (G を i 回2倍算した値 (i は u のLSBから数えた時のビット位置))を加算する。

【0157】

ステップS5で、 $c = X_v \bmod r$ を計算し、ステップS6でこの値が0になるかどうか判定し、0でなければステップS7で $d = [(f + cK_s) / u] \bmod r$ を計算し、ステップS8で d が0であるかどうか判定し、 d が0でなければ、ステップS9で c および d を電子署名データとして出力する。仮に、 r を160ビット長の長さであると仮定すると、電子署名データは320ビット長となる。

【0158】

ステップS6において、 c が0であった場合、ステップS3に戻って新たな乱数を生成し直す。同様に、ステップS8で d が0であった場合も、ステップS3に戻って乱数を生成し直す。30

【0159】

次に、公開鍵暗号方式を用いた電子署名の検証方法を、図20を用いて説明する。ステップS11で、 M をメッセージ、 p を標数、 a 、 b を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0 \pmod{p}$ ）、 G を楕円曲線上のベースポイント、 r を G の位数、 G および $K_s \times G$ を公開鍵 ($0 < K_s < r$) とする。ステップS12で電子署名データ c および d が $0 < c < r$ 、 $0 < d < r$ を満たすか検証する。これを満たしていた場合、ステップS13で、メッセージ M のハッシュ値を計算し、 $f = \text{Hash}(M)$ 40
) とする。次に、ステップS14で $h = 1 / d \bmod r$ を計算し、ステップS15で $h1 = fh \bmod r$ 、 $h2 = ch \bmod r$ を計算する。

【0160】

ステップS16において、既に計算した $h1$ および $h2$ を用い、点 $P = (X_p, Y_p) = h1 \times G + h2 \cdot K_s \times G$ を計算する。電子署名検証者は、ベースポイント G および $K_s \times G$ を知っているので、図19のステップS4と同様に楕円曲線上の点のスカラー倍の計算ができる。そして、ステップS17で点 P が無限遠点かどうか判定し、無限遠点でなければステップS18に進む（実際には、無限遠点の判定はステップS16ですべてしまう。つまり、 $P = (X, Y)$ 、 $Q = (X, -Y)$ の加算を行うと、 λ が計算できず、 $P + Q$ 50

が無限遠点であることが判明している)。ステップS18で X_{pmodr} を計算し、電子署名データ c と比較する。最後に、この値が一致していた場合、ステップS19に進み、電子署名が正しいと判定する。

【0161】

電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

【0162】

ステップS12において、電子署名データ c または d が、 $0 < c < r$ 、 $0 < d < r$ を満たさなかった場合、ステップS20に進む。また、ステップS17において、点 P が無限遠点であった場合もステップS20に進む。さらにまた、ステップS18において、 X_{pmodr} の値が、電子署名データ c と一致していなかった場合にもステップS20に進む。

【0163】

ステップS20において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。上述したように、署名付けやハッシュをとるだけでは改竄は可能であるが、検出により実質的に改竄できないことと同様の効果がある。

【0164】

上述した電子署名の生成、検証により、改竄された属性証明書の利用を防止することが可能となる。なお、属性証明書を適用したアクセス権限の確認処理に際しても、属性証明書の署名検証が実行される。この処理については後述する。

【0165】

次に、通信処理装置（ユーザデバイス）としてのエンドエンティティ（EE）の新規追加、および、エンドエンティティ（EE）に対するドメイン名属性証明書、およびホスト名属性証明書の発行シーケンスについて、図21乃至図23を参照して説明する。

【0166】

なお、図21乃至図22において、
新規EE：新規の通信処理装置としてホームサーバの管理下に追加するエンドエンティティ

ホームサーバ：属性証明書に基づく審査に基づいてホーム名前解決サーバを利用した名前解決を実行する中継サーバ、

ホーム名前解決サーバ：ホームサーバの利用する名前解決サーバ、

ドメイン名ARA：ドメイン名属性証明書登録局、

ドメイン名AA：ドメイン名属性証明書認証局、

である。

【0167】

まず、図21、ステップS201において、通信処理装置としての新規EE（エンドエンティティ）がネットワークに接続され、ステップS202において、ホームサーバに対して登録要求を出力する。この新規EEは、たとえば図11を参照して説明した構成を持ち、ネットワークインタフェース232（図11参照）を介してネットワークに接続する。

【0168】

ホームサーバは、新規EEからの登録要求に対して仮アドレスを割り当て（S203）、その後、新規EEとホームサーバ間で相互認証が実行（S204）される。この相互認証処理は、例えば先に図17を参照して説明したシーケンスに従って実行される。相互認証の成立を条件として、次ステップに進む。新規EEは、登録処理に必要な機器情報をホームサーバに送信（S205）し、ホームサーバは、受信情報の検証、審査を実行（S206）する。

【0169】

検証、審査の結果登録不可（S207：No）と判定されると、エラー処理（S208）を実行して処理終了となる。検証、審査の結果登録可（S207：Yes）と判定されると、登録可能通知を新規EEに送信（S209）し、新規EEは、登録可能通知を受信す

るとEE名(ホスト名)登録申請をホームサーバに送信(S210)し、ホームサーバは、希望EE名(ホスト名)を新規EEに対して要求(S211)し、新規EEは、希望EE名(ホスト名)をホームサーバに送信(S212)する。

【0170】

新規EEが希望EE名(ホスト名)をホームサーバに送信すると、ホームサーバは、EE名(ホスト名)未登録確認処理を実行(S213)する。これは、ステップS214以下の処理として実行され、ホームサーバからホーム名前解決サーバに対して希望EE名(ホスト名)が送信されて、ホーム名前解決サーバが希望EE名(ホスト名)の検索を実行し、未登録か否かを判定する。登録されている場合は、ステップS211に戻り、再度、希望EE名(ホスト名)を要求する。

10

【0171】

希望EE名(ホスト名)が登録されていない場合は、ステップS216に進み、登録可能通知をホームサーバに送信し、ホームサーバは、EE名(ホスト名)に対応するアドレス空間の割り当てを実行(S217)して、ステップS218において、決定したEE名(ホスト名)と、対応するアドレスとを新規登録EEに通知し、一方、ホーム名前解決サーバに対しても、決定したEE名(ホスト名)と、対応するアドレスを送信する。ホーム名前解決サーバは、ホスト名に対応するアドレス空間をデータベース(図14(b)参照)に登録する。

【0172】

次に、図22を参照して、エンドエンティティ(EE)が実行するドメイン名属性証明書(ドメイン名AC)の発行要求に対する処理手順について説明する。

20

【0173】

まず、ステップS221において、EE(エンドエンティティ)がホームサーバに対してドメイン名属性証明書(ドメイン名AC)の発行要求を出力する。ホームサーバは、EEからの要求を受信すると、EEとホームサーバ間で相互認証を実行(S222)する。この相互認証処理は、例えば先に図17を参照して説明したシーケンスに従って実行される。相互認証の成立を条件として、次ステップに進む。EEは、ドメイン名属性証明書(ドメイン名AC)発行処理に必要な機器情報、ホスト名(EE名)をホームサーバに送信(S223)し、ホームサーバは、受信情報の検証、審査を実行(S224)する。

【0174】

検証、審査の結果ドメイン名属性証明書(ドメイン名AC)発行不可(S225:No)と判定されると、エラー処理(S226)を実行して処理終了となる。検証、審査の結果、ドメイン名属性証明書(ドメイン名AC)発行可(S225:Yes)と判定されると、ステップS227において、ホームサーバは、ドメイン名属性証明書登録局(ARA)に対してドメイン名属性証明書(ドメイン名AC)の発行要求を行なう。この際、ホームサーバの公開鍵証明書(PKC)と、EEの機器情報、ホスト名(EE名)、ドメイン名を付加データとして送信する。

30

【0175】

ドメイン名属性証明書登録局(ARA)は、発行要求に基づいて、属性証明書発行ポリシーに従った審査を実行して、発行条件を満足すると判断すると、ステップS228において、ドメイン名属性証明書認証局(AA)に対して、ホームサーバの公開鍵証明書(PKC)と、EEの機器情報、ホスト名(EE名)、ドメイン名を通知するとともに、ドメイン名属性証明書発行要求を行なう。

40

【0176】

ドメイン名属性証明書認証局(AA)は、ステップS229において、ホームサーバの公開鍵証明書(PKC)と、登録済みドメイン名に基づいて、ドメイン名属性証明書を生成して、ドメイン名属性証明書登録局(ARA)に送信する。ここで生成するドメイン名属性証明書は、先に、図7(a)を参照して説明した構成を持ち、属性情報フィールドにドメイン名が格納され、ドメイン名属性証明書認証局(AA)の秘密鍵による署名がなされたものである。

50

【0177】

ドメイン名属性証明書登録局（A R A）は、受信したドメイン名属性証明書をホームサーバに送信（S 2 3 0）し、ホームサーバは、ステップS 2 3 1において、ドメイン名属性証明書（A C）をエンドエンティティ（E E）に送信し、一方、ホーム名前解決サーバに対しても、ホスト名、ドメイン名属性証明書（A C）のコピーを送信する。

【0178】

次に、図23を参照して、エンドエンティティ（E E）が実行するホスト名属性証明書（ホスト名A C）の発行要求に対する処理手順について説明する。

【0179】

なお、図23において、
新規E E：新規の通信処理装置としてホームサーバの管理下に追加するエンドエンティティ

10

ホームサーバ：属性証明書に基づく審査に基づいてホーム名前解決サーバを利用した名前解決を実行する中継サーバ、

ホーム名前解決サーバ：ホームサーバの利用する名前解決サーバ、

ホスト名A R A：ホスト名属性証明書登録局、

ホスト名A A：ホスト名属性証明書認証局、

である。

【0180】

まず、ステップS 2 4 1において、E E（エンドエンティティ）がホームサーバに対して
ホスト名属性証明書（ホスト名A C）の発行要求を出力する。ホームサーバは、E Eからの
要求を受信すると、E Eとホームサーバ間で相互認証が実行（S 2 4 2）される。この
相互認証処理は、例えば先に図17を参照して説明したシーケンスに従って実行される。
相互認証の成立を条件として、次ステップに進む。E Eは、ホスト名属性証明書（ホスト
名A C）発行処理に必要な機器情報、ホスト名（E E名）をホームサーバに送信（S
2 4 3）し、ホームサーバは、受信情報の検証、審査を実行（S 2 4 4）する。

20

【0181】

検証、審査の結果ホスト名属性証明書（ホスト名A C）発行不可（S 2 4 5：N o）と判定
されると、エラー処理（S 2 4 6）を実行して処理終了となる。検証、審査の結果、ホ
スト名属性証明書（ホスト名A C）発行可（S 2 4 5：Y e s）と判定されると、ステッ
プS 2 4 7において、ホームサーバは、ホスト名属性証明書登録局（A R A）に対してホ
スト名属性証明書（ホスト名A C）の発行要求を行なう。この際、ホームサーバの公開鍵
証明書（P K C）と、E Eの機器情報、ホスト名（E E名）を付加データとして送信する
。

30

【0182】

ホスト名属性証明書登録局（A R A）は、発行要求に基づいて、ポリシーに従った審査を
実行して、発行条件を満足すると判断すると、ステップS 2 4 8において、ホスト名属性
証明書認証局（A A）に対して、ホームサーバの公開鍵証明書（P K C）と、E Eの機器
情報、ホスト名（E E名）、ホスト名とともに、ホスト名属性証明書発行要求を行なう。

【0183】

ホスト名属性証明書認証局（A A）は、ステップS 2 4 9において、ホームサーバの公開
鍵証明書（P K C）と、登録済みホスト名に基づいて、ホスト名属性証明書を生成して、
ホスト名属性証明書登録局（A R A）に送信する。ここで生成するホスト名属性証明書は
、先に、図7（b）を参照して説明した構成を持ち、属性情報フィールドにホスト名が格
納され、ホスト名属性証明書認証局（A A）の秘密鍵による署名がなされたものである。

40

【0184】

ホスト名属性証明書登録局（A R A）は、受信したホスト名属性証明書をホームサーバに
送信（S 2 5 0）し、ホームサーバは、ステップS 2 5 1において、ホスト名属性証明書
（A C）をエンドエンティティ（E E）に送信し、一方、ホーム名前解決サーバに対しても、
ホスト名、ホスト名属性証明書（A C）のコピーを送信する。

50

【0185】

なお、上記処理において、ホスト名属性証明書（AC）を受領したエンドエンティティ（EE）は、その署名を検証してドメイン名属性証明書（AC）の改竄がないことを確認した後、自己のメモリに格納する。

【0186】

（3-3）アクセス許可情報の登録および削除処理

次に、アクセス許可情報の登録および削除処理について説明する。例えば図13に示した構成において、エンドエンティティ（EE）としてのユーザデバイス311は、自身に対するアクセス要求について接続を許可するアクセス要求元グループを、中継サーバ1（ホームサーバ1）313に登録することができる。一方、ユーザデバイス321は、自身に対するアクセス要求について接続を許可するアクセス要求元グループを、中継サーバ2（ホームサーバ2）323に登録することができる。

【0187】

中継サーバ1、313は、自己の管理ユーザデバイス、すなわち名前解決サーバ312を適用した名前解決処理サービスを提供可能な端末（例えば図13ではユーザデバイス311）から、自端末（ユーザデバイス311）に対するアクセス要求許可グループ情報を受領して、その情報登録を行う。

【0188】

中継サーバ1、313は、登録情報、およびアクセス要求元から提示されるドメイン名属性証明書、ホスト名属性証明書、その他のグループ属性証明書に基づいてアクセス可否を判定し、アクセス要求元がアクセスが許可されたグループに属している場合にのみ名前解決処理を行なってホスト名からアドレスを取得してアクセス要求元に通知する。

【0189】

まず、図24を参照してユーザデバイスであるエンドエンティティ（EE）が、自デバイスの名前解決処理を実行するホームサーバに対してアクセス許可グループ情報を登録するシーケンスについて説明する。なお、図24において、
EE：アクセス許可情報の登録を要求するエンドエンティティ（ユーザデバイス）
ホームサーバ：EEのホスト名に基づく名前解決をアクセス要求元から提示される属性証明書、および登録されたアクセス許可情報に基づいて判定するホームサーバ
許可グループデータベース：アクセス許可情報の登録用データベース
である。

【0190】

まず、ステップS301において、ユーザがユーザデバイスであるエンドエンティティ（EE）に対して、EEのインタフェースを介して許可グループ情報の登録開始要求を入力する。ステップS302において、EEは、自身の名前解決処理の実行判定を行なうホームサーバに対して許可グループ情報登録要求を出力する。

【0191】

次に、ステップS303において、ホームサーバとエンドエンティティ（EE）間において相互認証を実行する。この相互認証処理は、例えば先に図17を参照して説明したシーケンスに従って実行する。相互認証の成立を条件として、次ステップに進む。ステップS304において、EEは、登録処理に必要な情報、すなわち、アクセスを許容するグループ情報、アクセス許可期限などの情報をホームサーバに送信する。

【0192】

ホームサーバは、受信情報に基づいて、許可グループデータベース（DB）に対する登録処理を実行（S305）し、登録後、登録完了通知をエンドエンティティ（EE）に送信（S306）して、登録処理が終了する。

【0193】

許可グループデータベースの構成例を図25に示す。図25の例は、エンドエンティティ（e-e-a）と、エンドエンティティ（e-e-b）の2つのEEに対するアクセス許可グループが登録された例を示している。

【0194】

エンドエンティティ (e e - a) については、A社の機器、ユーザについて、5月5日まで、鈴木家の機器、ユーザに対して無期限、a b c . n e t ドメイン内の機器に対して設定から48時間内のアクセスを許可する情報が登録されている。エンドエンティティ (e e - b) は、A社アメリカ支店の機器、ユーザについて、提示される属性証明書の有効期限内、X大学理学部の機器、ユーザに対して3月31日まで、e e - s . h o m e 2 . a b c . n e t のホスト名機器に対して設定から4月8日までのアクセスを許可する情報が登録されている。

【0195】

図25に示す許可グループデータベースを持つホームサーバは、アクセス要求元から提示される属性証明書に基づいてアクセス要求元が、アクセス許可グループに属するか否かを判定し、属すると判定された場合に名前解決処理により、アクセス要求元のデバイス (E E) のホスト名からアドレスを取得して、アクセス要求元に通知する。

【0196】

次に、図26を参照してアクセス許可グループ情報の削除シーケンスについて説明する。なお、図26において、

EE: アクセス許可情報の登録を要求するエンドエンティティ (ユーザデバイス)
ホームサーバ: EEのホスト名に基づく名前解決をアクセス要求元から提示される属性証明書、および登録されたアクセス許可情報に基づいて判定するホームサーバ
許可グループデータベース: アクセス許可情報の登録用データベース

【0197】

まず、ステップS311において、ユーザがユーザデバイスであるエンドエンティティ (EE) に対して、EEのインタフェースを介して許可グループ情報の削除開始要求を入力する。ステップS312において、EEは、自身の名前解決処理の実行判定を行なうホームサーバに対して許可グループ情報削除要求を出力する。

【0198】

次に、ステップS313において、ホームサーバとエンドエンティティ (EE) 間において、相互認証が実行される。この相互認証処理は、例えば先に図17を参照して説明したシーケンスに従って実行される。相互認証の成立を条件として、次ステップに進む。ステップS314において、EEは、削除処理に必要な情報、すなわち、削除を実行するグループ情報をホームサーバに送信する。

【0199】

ホームサーバは、受信情報に基づいて、許可グループデータベース (DB) の登録情報の削除処理を実行 (S315) し、削除後、削除完了通知をエンドエンティティ (EE) に送信 (S316) して、登録処理が終了する。

【0200】

(3-4) アクセス許可判定処理

次に、ネットワークを介した通信において、上述したアクセス許可グループデータベースを適用してアクセスの制限を行なう処理シーケンスについて説明する。

【0201】

図27は、アクセス元EEからアクセス先EEに対してネットワークを介したアクセスを実行する際のシーケンスを示した図である。図27において、

アクセス先EE: アクセス先としてのエンドエンティティ (ユーザデバイス)
ホーム名前解決サーバ: アクセス先EEに関するホスト名からアドレスの取得処理 (名前解決処理) を行なうサーバ
アクセス先ホームサーバ: アクセス先EEのホスト名に基づく名前解決をアクセス要求元から提示される属性証明書、および登録されたアクセス許可情報に基づいて判定するホームサーバ
アクセス元EE所属ドメインホームサーバ: アクセス元EEの管理サーバであり、ネット

10

20

30

40

50

ワークを介する通信時に中継サーバとして機能し、アクセス先ホームサーバのアドレスをアクセス元E Eに通知する処理を行なうホームサーバ
アクセス元E E：アクセス元としてのエンドエンティティ（ユーザデバイス）である。

【0202】

まず、ステップS 3 2 1において、アクセス元E Eは、アクセス元E E所属ドメインホームサーバに対して、アクセス先E Eの所属ドメイン名を送信する。ステップS 3 2 2において、アクセス元E E所属ドメインホームサーバは、自己の管理範囲または、上位のサーバの管理する名前解決サーバを適用して、受信ドメイン名に対応するアクセス先のホームサーバのIPアドレスをアクセス元E Eに通知する。

10

【0203】

ドメイン名に基づく、アクセス先ホームサーバのIPアドレスのアクセス元E Eに対する通知処理の詳細シーケンスについて、図28を参照して説明する。図28において、SPは、アクセス元E E所属ドメインサーバの上位ドメインのサービスプロバイダ（SP）であり、SP名前解決サーバは、そのSPの適用する名前解決サーバである。

【0204】

アクセス元E E所属ドメインホームサーバが、アクセス元E Eからドメイン名を受信すると、ステップS 3 5 1において、アクセス元E E所属ドメインホームサーバは、アクセス元E E所属ドメイン名前解決サーバに対して、ドメイン名に対応するアドレス取得を要求する。

20

【0205】

アクセス元E E所属ドメイン名前解決サーバは、たとえば先に図14を参照して説明したデータベースに基づいてドメインが登録されているかを判定し、存在すれば（S 3 5 2：Yes）、データベースからアドレスを取得してステップS 3 5 7で、ドメイン名に対応するホームサーバのIPアドレスをアクセス元E E所属ドメインホームサーバに送信し、アクセス元E E所属ドメインホームサーバからアクセス要求元E Eにアドレス情報が送信される。

【0206】

一方、アクセス元E E所属ドメイン名前解決サーバのデータベースにドメインが登録されていない（S 3 5 2：No）場合は、上位ドメインのサービスプロバイダ（SP）にドメインを送信し、名前解決を要求（S 3 5 3）する。サービスプロバイダ（SP）は、SP名前解決サーバに対して、ドメイン名検索を要求（S 3 5 4）し、SP名前解決サーバは、ドメインに対応するホームサーバのIPアドレスを取得して、サービスプロバイダ（SP）に送信（S 3 5 5）し、サービスプロバイダ（SP）からアクセス元E E所属ドメインホームサーバ（S 3 5 6）、アクセス元E E所属ドメインホームサーバからアクセス要求元E Eにアドレス情報が送信（S 3 5 7）される。

30

【0207】

なお、図28の例では、ドメイン名に対応するアドレス取得を1つのサービスプロバイダ（SP）に問い合わせる例を示しているが、必要に応じて、さらに上位、あるいは他のドメインのSPに対して、アドレス取得が実行されるまで再帰的に問い合わせを実行し、必要なアドレス情報を取得する。

40

【0208】

図27に戻り、説明を続ける。ステップS 3 2 2において、上述した処理により、アクセス元E Eが、アクセス先ホームサーバのIPアドレスを取得すると、次に、ステップS 3 2 3において、アクセス元E Eは、受信したアクセス先のホームサーバのIPアドレスに従って、アクセス先ホームサーバにアクセスして、相互認証を実行（S 3 2 4）する。相互認証処理は、例えば先に図17を参照して説明したシーケンスに従って実行される。相互認証の成立を条件として、次ステップに進む。アクセス元E Eは、ステップS 3 2 5において、アクセス先ホームサーバに自己の属性証明書を送付して、アクセス先E Eのホスト名からのアドレス取得、すなわち名前解決処理を要求する。

50

【0209】

属性証明書を受領したアクセス先ホームサーバは、属性証明書の検証、審査を実行する。属性証明書の検証とは、署名検証による改竄有無の検証であり、審査は、前述の許可グループデータベースを参照して、属性証明書によって証明されたグループが許可グループとして登録されているか否かの審査である。

【0210】

属性証明書の検証処理の詳細について、図29乃至図31を参照して説明する。まず、属性証明書(AC)と公開鍵証明書(PKC)との関連確認処理について、図29を参照して説明する。図29のフローは、属性証明書(AC)の検証を実行する際に行なわれる属性証明書(AC)に関連する公開鍵証明書(PKC)の確認処理である。

10

【0211】

確認対象の属性証明書(AC)がセット(S421)されると、属性証明書のAC保持者の公開鍵証明書情報(ホルダー)フィールドを抽出(S422)し、抽出した公開鍵証明書情報(ホルダー)フィールド内に格納された公開鍵証明書の発行者情報(PKC発行者)、公開鍵証明書シリアル番号(PKCシリアル)を確認(S423)し、公開鍵証明書の発行者情報(PKC発行者)、公開鍵証明書シリアル番号(PKCシリアル)に基づいて公開鍵証明書(PKC)を検索(S424)して、属性証明書(AC)に関連付けられた公開鍵証明書(PKC)を取得(S425)する。

【0212】

図29に示すように、属性証明書(AC)と公開鍵証明書(PKC)とは、属性証明書に格納された公開鍵証明書情報(ホルダー)フィールド内の公開鍵証明書発行者情報(PKC発行者)、および公開鍵証明書シリアル番号(PKCシリアル)により関連付けがなされている。

20

【0213】

次に、図30を参照して属性証明書(AC)の検証処理について説明する。まず、検証対象となる属性証明書(AC)をセット(S451)し、属性証明書(AC)格納情報に基づいて、属性証明書(AC)の所有者および署名者を特定(S452)する。さらに、属性証明書(AC)の所有者の公開鍵証明書を直接あるいはリポジトリなどから取得(S453)して、公開鍵証明書の検証処理を実行(S454)する。

【0214】

図31を参照して公開鍵証明書(PKC)の検証処理について説明する。図31に示す公開鍵証明書(PKC)の検証は、下位から上位へ証明書連鎖をたどって最上位の公開鍵証明書までの連鎖情報を取得して、最上位(ルートCA)までの公開鍵証明書の署名検証を行なう連鎖検証処理フローである。まず、検証対象となる公開鍵証明書(PKC)をセット(S471)し、公開鍵証明書(PKC)格納情報に基づいて、公開鍵証明書(PKC)署名者を特定(S472)する。さらに、検証対象となる証明書連鎖の最上位の公開鍵証明書であるかを判定(S473)し、最上位でない場合は、最上位公開鍵証明書を直接あるいはリポジトリなどから取得(S474)する。最上位公開鍵証明書が取得されセット(S475)されると、署名検証に必要な検証鍵(公開鍵)を取得(S476)し、検証対象の署名が自己署名であるか否かを判定し(S477)、自己署名でない場合は、下位PKCをセット(S479)して、上位の公開鍵証明書から取得した検証鍵(公開鍵)に基づいて署名検証を実行(S480)する。なお、ステップS477における自己署名判定において、自己署名の場合は自己の公開鍵を検証鍵とした検証を実行(S478)し、ステップS481に進む。

30

40

【0215】

署名検証に成功した場合(S481:Yes)は、目的とするPKCの検証が完了したか否かを判定(S482)し、完了している場合は、PKC検証を終了する。完了していない場合は、ステップS476に戻り、署名検証に必要な検証鍵(公開鍵)の取得、下位の公開鍵証明書の署名検証を繰り返し実行する。なお、署名検証に失敗した場合(S481:No)は、ステップS483に進み、エラー処理、例えばその後の手続きを停止する等

50

の処理を実行する。

【0216】

図30に戻り、属性証明書検証処理の説明を続ける。図31で説明した公開鍵証明書の検証に失敗した場合（S455でNo）は、ステップS456に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合（S455でYes）は、属性証明書（AC）の署名者に対応する公開鍵証明書を直接あるいはリポジトリなどから取得（S457）して、属性証明書（AC）の署名者に対応する公開鍵証明書の検証処理を実行（S458）する。

【0217】

属性証明書（AC）の署名者に対応する公開鍵証明書の検証に失敗した場合（S459でNo）は、ステップS460に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合（S459でYes）は、属性証明書（AC）の署名者に対応する公開鍵証明書から公開鍵を取り出し（S461）て、取り出した公開鍵を用いて属性証明書（AC）の署名検証処理を実行（S462）する。署名検証に失敗した場合（S463でNo）は、ステップS464に進み、エラー処理を行なう。例えばその後の処理を中止する。署名検証に成功した場合（S463でYes）は、属性証明書検証を終了し、その後の処理、すなわち属性証明書の属性情報として登録されたグループ情報を取得し、取得したグループ情報が、許可グループデータベース（図25参照）にアクセス許可グループとして登録されているか否かの審査処理を実行する。

【0218】

審査処理の詳細について、図32を参照して説明する。ステップS491の判定は、図29乃至図31を参照して説明した属性証明書署名検証の検証結果判定ステップであり、検証不成立の場合は、この時点で、ステップS499に進み、検証・審査不合格応答をアクセス元EEに対して行なうことになる。

【0219】

ステップS491の判定が、Yes、すなわち、属性証明書署名検証に成功し、属性証明書の改竄がないことが確認されると、ステップS492、S493において、属性証明書から発行者情報、属性情報（グループ情報）を取得する。このグループ情報は、先に図6を参照して説明したように、さまざまな機器グループ、ユーザグループ、ドメイン、ホストなどによって定義されるグループであり、例えばグループ情報としてのグループID、ドメイン名、ホスト名などによって構成される情報である。

【0220】

ステップS494で、アクセス先ホームサーバは、アクセス先EE名（ホスト名）を検索キーとして許可グループデータベース（図25参照）の検索を実行し、許可グループデータベースは、アクセス先EE名（ホスト名）の許可グループリストを検索結果としてホームサーバに応答する（S495）。ホームサーバは、受信リストにグループ属性証明書から取得したグループ情報がアクセス許可グループとして含まれるか否かを判定（S497）し、存在した場合は、ステップS498において、名前解決サーバに対する名前解決処理要求（図27のステップS329-）を行なうことになる。一方、受信リストにグループ属性証明書から取得したグループ情報がアクセス許可グループとして含まれていない場合は、ステップS499に進み、検証・審査不合格応答をアクセス元EEに対して行なうことになる。

【0221】

図27のシーケンス図に戻って説明を続ける。ステップS326では、上述したグループ属性証明書（Gp. AC）の検証後、属性証明書の属性情報として登録されたグループ情報を取得し、取得したグループ情報が、許可グループデータベース（図25参照）にアクセス許可グループとして登録されているか否かの審査処理を実行する。

【0222】

上述のグループ属性証明書の検証、および審査処理において合格、すなわち、グループ属性証明書が改竄のない正当な証明書であり、属性証明書の属性情報フィールドに記録され

たグループ情報が許可グループデータベース（図25参照）にアクセス許可グループとして登録されている場合（S327：Yes）には、ステップS329に進み、ホーム名前解決サーバに対してアクセス先EE名（ホスト名）を出力する。ホーム名前解決サーバは、先に図14（b）を参照して説明したデータベースを持ち、アクセス先EE名（ホスト名）に対応するアドレスを取得（S330）して、アクセス先ホームサーバに応答する。ステップS331において、アクセス先ホームサーバは、取得アドレスをアクセス元EEに通知し、アクセス元EEは、取得アドレスに基づいて、アクセス先EEへのアクセスを実行する。

【0223】

一方、ステップS327の判定がNo、すなわち、グループ属性証明書の検証、および審査処理において不合格、すなわち、グループ属性証明書が改竄のない正当な証明書であることが証明されなかった場合、あるいは、属性証明書の属性情報フィールドに記録されたグループ情報が許可グループデータベース（図25参照）にアクセス許可グループとして登録されていない場合には、ステップS328において、名前解決処理を実行しない、すなわち、名前解決不許可通知をアクセス元EEに送信する。この場合、アクセス元EEは、アクセス先EEのアドレスを取得することができないので、アクセスが実行できないこととなる。

【0224】

上述の属性証明書に基づくアクセス可否判定処理において実行されるシーケンスについて、図33を参照して総括して説明する。

【0225】

図33のユーザデバイス321がアクセス元EEであり、ユーザデバイス311がアクセス先EEであり、（1）から（7）の順に処理が進められる。まず、（1）において、ユーザデバイス（アクセス元EE）321は、中継サーバ2（ホームサーバ2）323に対してアクセス先EEのドメイン名を送信し、中継サーバ2（ホームサーバ2）323が名前解決サーバ322、あるいは上位ドメインのサービスプロバイダ341、あるいはさらに他のサーバを介してアクセス先EEのドメイン内のホームサーバ、すなわち中継サーバ1（ホームサーバ1）313に対応するアドレスを取得して、（2）で取得アドレス情報をユーザデバイス（アクセス元EE）321に応答する。

【0226】

ユーザデバイス（アクセス元EE）321は、取得アドレスにしたがって、中継サーバ1（ホームサーバ1）313に対してアクセスし、属性証明書を送付するとともにユーザデバイス（アクセス先EE）311のホスト名についての名前解決処理の要求を行なう。中継サーバ1（ホームサーバ1）313は、属性証明書の検証、および許可グループデータベース314のデータに基づく審査を実行し、検査、審査の双方が成立したことを条件として、（4）において、名前解決サーバ312を適用してユーザデバイス（アクセス先EE）311のホスト名の名前解決処理を実行し、（5）でユーザデバイス（アクセス先EE）311のホスト名に対応するアドレスを取得して、（6）で、取得アドレスをユーザデバイス（アクセス元EE）321に通知する。

【0227】

次に、（7）の処理として、ユーザデバイス（アクセス元EE）321は、取得アドレスに基づいて、ユーザデバイス（アクセス先EE）311に対するアクセスを実行する。

【0228】

このように、アクセス要求元が、アクセス先のユーザデバイス（エンドエンティティ）が設定したアクセス許可グループに属することが確認されることがアクセス許可条件となり、不特定多数のデバイスからのアクセスが排除可能となる。また、属性証明書に基づく検証、審査が実行されるので、確実な審査が可能となる。

【0229】

（3-5）アドレス更新処理

上述の手法により、アクセスをアクセス先EEの認定したグループのメンバーに限定する

ことが可能となる。エンドエンティティ（ユーザデバイス）のアドレスが固定的であると、一度取得したアドレス情報に基づいて、その後、アクセス許可グループから除外された場合でもアクセスされる可能性がある。このような事態を防止するため、アドレスを動的に変更するアドレス更新処理について、以下説明する。

【0230】

まず、図34のシーケンス図に基づいて、ホームサーバが、エンドエンティティのアドレス更新スケジュールを管理し、スケジュールに従って、エンドエンティティ（EE）のアドレスの更新処理を実行するシーケンスについて説明する。図34において、

更新対象EE：アドレスの更新を実行するエンドエンティティ（ユーザデバイス）

ホームサーバ：更新対象EEのホスト名に基づく名前解決をアクセス要求元から提示される属性証明書、および登録されたアクセス許可情報に基づいて判定するホームサーバ

ホーム名前解決サーバ：更新対象EEに関するホスト名からアドレスの取得処理（名前解決処理）を行なうサーバ

である。

【0231】

まず、ステップS511において、ホームサーバは、アドレス更新時期スケジューリングに従って、更新時期のエンドエンティティを選択し更新対象EEを決定（S512）する。アドレス更新時期スケジュールデータは、例えば所定日数ごとの一定期間サイクルの更新実行スケジュールをエンドエンティティごとの管理データとして構成する。

【0232】

更新対象のエンドエンティティが決定すると、ステップS513において、アドレス更新通知が更新対象EEに通知され、ステップS514でホームサーバと、更新対象EE間の相互認証を実行する。相互認証処理は、例えば先に図17を参照して説明したシーケンスに従って実行される。相互認証の成立を条件として、次ステップに進む。

【0233】

ステップS515において、更新対象EEは、自己のグループ属性証明書をホームサーバに提示する。グループ属性証明書は、例えばドメイン名属性証明書、ホスト名属性証明書、あるいはその他のグループ情報を属性情報として格納したグループ属性証明書である。

【0234】

ステップS516において、ホームサーバは、更新対象EEから受信したグループ属性証明書（グループAC）の検証、審査を実行する。検証、審査処理は、先に図29乃至図32を参照して説明した処理に準ずる処理である。ただし、ここでの審査は、許可グループデータベースに対応するグループのアクセス許可がなされているか否かではなく、許可グループデータベースに更新対象EEの対応エントリが存在するか否かの審査となる。存在する場合は、審査成立とする。

【0235】

グループACの検証、審査が不成立の場合（S517：No）は、エラー処理（S518）として、例えば更新対象EEに対してエラーメッセージの送付等が行なわれる。グループACの検証、審査が成立の場合（S517：Yes）は、ステップS519において、更新対象EEのアドレスが更新され、新アドレスが更新対象EEに対して送信され、更新対象EEにおいて、新アドレスに基づくアドレス更新が実行（S520）されて、更新完了通知がホームサーバに通知される。

【0236】

ホームサーバは、更新対象EEの新アドレスをホーム名前解決サーバに、更新対象EE名（ホスト名）とともに通知（S521）し、ホーム名前解決サーバは、名前解決データベース（図14（b）参照）を更新（S522）する。

【0237】

次に、図35のシーケンス図に基づいて、更新対象エンドエンティティ（EE）自身が、自己のアドレス更新スケジュールを管理し、スケジュールに従ってアドレス更新処理を実行するシーケンスについて説明する。図35において、

10

20

30

40

50

更新対象 E E：アドレスの更新を実行するエンドエンティティ（ユーザデバイス）
ホームサーバ：更新対象 E E のホスト名に基づく名前解決をアクセス要求元から提示される属性証明書、および登録されたアクセス許可情報に基づいて判定するホームサーバ
ホーム名前解決サーバ：更新対象 E E に関するホスト名からアドレスの取得処理（名前解決処理）を行なうサーバである。

【0238】

まず、ステップ S 5 3 1 において、更新対象 E E は、アドレス更新時期スケジューリングに従って、更新時期の到来を確認し、ステップ S 5 3 2 において、アドレス更新要求をホームサーバに送信し、ステップ S 5 3 3 でホームサーバと、更新対象 E E 間の相互認証を実行する。相互認証処理は、例えば先に図 1 7 を参照して説明したシーケンスに従って実行される。相互認証の成立を条件として、次ステップに進む。

【0239】

ステップ S 5 3 4 において、更新対象 E E は、自己のグループ属性証明書をホームサーバに提示する。グループ属性証明書は、例えばドメイン名属性証明書、ホスト名属性証明書、あるいはその他のグループ情報を属性情報として格納したグループ属性証明書である。

【0240】

ステップ S 5 3 5 において、ホームサーバは、更新対象 E E から受信したグループ属性証明書（グループ A C）の検証、審査を実行する。検証、審査処理は、先に図 2 9 乃至図 3 2 を参照して説明した処理に準ずる処理である。ただし、ここでの審査は、許可グループデータベースに対応するグループのアクセス許可がなされているか否かではなく、許可グループデータベースに更新対象 E E の対応エントリが存在するか否かの審査となる。存在する場合は、審査成立とする。

【0241】

グループ A C の検証、審査が不成立の場合（S 5 3 6：No）は、エラー処理（S 5 3 7）として、例えば更新対象 E E に対してエラーメッセージの送付等が行なわれる。グループ A C の検証、審査が成立の場合（S 5 3 6：Yes）は、ステップ S 5 3 8 において、更新対象 E E のアドレスが更新され、新アドレスが更新対象 E E に対して送信され、更新対象 E E において、新アドレスに基づくアドレス更新が実行（S 5 3 9）されて、更新完了通知がホームサーバに通知される。

【0242】

ホームサーバは、更新対象 E E の新アドレスをホーム名前解決サーバに、更新対象 E E 名（ホスト名）とともに通知（S 5 4 0）し、ホーム名前解決サーバは、名前解決データベース（図 1 4（b）参照）を更新（S 5 4 1）する。

【0243】

次に、ホームサーバおよびエンドエンティティの属するドメイン名に対応するアドレスの更新処理シーケンスについて説明する。

【0244】

まず、図 3 6 を参照して、ホームサーバのドメイン名に対応するアドレス管理を実行するサービスプロバイダ（S P）が、アドレス更新スケジュールを管理し、スケジュールに従って、ホームサーバおよびエンドエンティティの属するドメイン名に対応するアドレスの更新処理を実行するシーケンスについて説明する。図 3 6 において、

更新対象ドメイン内 E E：ドメイン名対応アドレスの更新を実行するドメイン内のエンドエンティティ（ユーザデバイス）

更新対象ドメイン名前解決サーバ：ドメイン名対応アドレスの更新を実行するドメイン内の名前解決サーバ

更新対象ホームドメインホームサーバ：ドメイン名対応アドレスの更新を実行するドメイン内のホームサーバ

S P：ドメイン名に対応するアドレス管理を実行するサービスプロバイダ（S P）

S P 名前解決サーバ：S P の管理する名前解決サーバであり、ドメイン名に対応するアド

レスの取得処理を実行するデータ（図14（a）参照）を有するである。

【0245】

まず、ステップS551において、サービスプロバイダ（SP）は、アドレス更新時期スケジュールに従って、更新時期のドメインを選択し更新対象ドメインを決定（S552）する。アドレス更新時期スケジュールデータは、例えば所定日数ごとの一定期間サイクルの更新実行スケジュールをドメインごとの管理データとして構成する。

【0246】

更新対象のドメインが決定すると、ステップS553において、アドレス空間更新通知が更新対象ドメインホームサーバに通知され、ステップS554でサービスプロバイダ（SP）と、更新対象ドメインホームサーバ間の相互認証を実行する。相互認証処理は、例えば先に図17を参照して説明したシーケンスに従って実行される。相互認証の成立を条件として、次ステップに進む。

【0247】

ステップS555において、更新対象ドメインホームサーバは、自己のグループ属性証明書をサービスプロバイダ（SP）に提示する。グループ属性証明書は、例えばドメイン名属性証明書、あるいはその他のグループ情報を属性情報として格納したグループ属性証明書である。

【0248】

ステップS556において、サービスプロバイダ（SP）は、更新対象ドメインホームサーバから受信したグループ属性証明書（グループAC）の検証、審査を実行する。検証、審査処理は、先に図29乃至図32を参照して説明した処理に準ずる処理である。ただし、ここでの審査は、許可グループデータベースに対応するグループのアクセス許可がなされているか否かではなく、許可グループデータベースに更新対象ドメインホームサーバの対応エントリが存在するか否かの審査となる。存在する場合は、審査成立とする。

【0249】

グループACの検証、審査が不成立の場合（S557：No）は、エラー処理（S558）として、例えば更新対象ドメインホームサーバに対してエラーメッセージの送付等が行なわれる。グループACの検証、審査が成立の場合（S557：Yes）は、ステップS559において、更新対象ドメインに対応する新アドレス空間の割り当てを実行する。

【0250】

次に、サービスプロバイダ（SP）は、更新対象ドメインに対応する新アドレス空間を更新対象ドメインホームサーバに通知し、さらに、SP名前解決サーバに、ドメイン名とともに新アドレス空間データを通知（S560）する。SP名前解決サーバは、名前解決データベース（図14（a）参照）を更新（S561）する。

【0251】

さらに、更新対象ドメインホームサーバは、新アドレス空間通知を更新対象ドメイン名前解決サーバに通知（S562）し、更新対象ドメイン名前解決サーバは、名前解決データベース（図14（b）参照）を更新（S563）して、更新完了通知を更新対象ドメインホームサーバに送信する。更新対象ドメインホームサーバは、さらに、自己の管理ユーザデバイスであるエンドエンティティである更新対象ドメイン内EEに対して、更新された新アドレスを通知（S564）し、更新対象ドメイン内EEにおいて、新アドレスに基づくアドレス更新が実行（S565）されて、更新完了通知が更新対象ドメインホームサーバに通知され、更新処理が終了する。

【0252】

次に、図37を参照して、ホームサーバ自身がドメイン名に対応するアドレス管理を実行して、スケジュールに従って、ホームサーバおよびエンドエンティティの属するドメイン名に対応するアドレスの更新処理を実行するシーケンスについて説明する。図37において、

更新対象ドメイン内EE：ドメイン名対応アドレスの更新を実行するドメイン内のエンド

エンティティ (ユーザデバイス)

更新対象ドメイン名前解決サーバ：ドメイン名対応アドレスの更新を実行するドメイン内の名前解決サーバ

更新対象ホームドメインホームサーバ：ドメイン名対応アドレスの更新を実行するドメイン内のホームサーバ

SP：ドメイン名に対応するアドレス管理を実行するサービスプロバイダ (SP)

SP名前解決サーバ：SPの管理する名前解決サーバであり、ドメイン名に対応するアドレスの取得処理を実行するデータ (図14 (a) 参照) を有する

である。

【0253】

10

まず、ステップS571において、更新対象ドメインホームサーバは、アドレス更新時期スケジューリングに従って、更新時期の到来を確認すると、アドレス更新要求をサービスプロバイダ (SP) に通知 (S572) する。ステップS573でサービスプロバイダ (SP) と、更新対象ドメインホームサーバ間の相互認証を実行する。相互認証処理は、例えば先に図17を参照して説明したシーケンスに従って実行される。相互認証の成立を条件として、次ステップに進む。

【0254】

ステップS574において、更新対象ドメインホームサーバは、自己のグループ属性証明書をサービスプロバイダ (SP) に提示する。グループ属性証明書は、例えばドメイン名属性証明書、あるいはその他のグループ情報を属性情報として格納したグループ属性証明書である。 20

【0255】

ステップS575において、サービスプロバイダ (SP) は、更新対象ドメインホームサーバから受信したグループ属性証明書 (グループAC) の検証、審査を実行する。検証、審査処理は、先に図29乃至図32を参照して説明した処理に準ずる処理である。ただし、ここでの審査は、許可グループデータベースに対応するグループのアクセス許可がなされているか否かではなく、許可グループデータベースに更新対象ドメインホームサーバの対応エントリが存在するか否かの審査となる。存在する場合は、審査成立とする。

【0256】

グループACの検証、審査が不成立の場合 (S576：No) は、エラー処理 (S577 30) として、例えば更新対象ドメインホームサーバに対してエラーメッセージの送付等が行なわれる。グループACの検証、審査が成立の場合 (S576：Yes) は、ステップS578において、更新対象ドメインに対応する新アドレス空間の割り当てを実行する。

【0257】

次に、サービスプロバイダ (SP) は、更新対象ドメインに対応する新アドレス空間を更新対象ドメインホームサーバに通知し、さらに、SP名前解決サーバに、ドメイン名とともに新アドレス空間データを通知 (S579) する。SP名前解決サーバは、名前解決データベース (図14 (a) 参照) を更新 (S580) する。

【0258】

さらに、更新対象ドメインホームサーバは、新アドレス空間通知を更新対象ドメイン名前 40
解決サーバに通知 (S581) し、更新対象ドメイン名前解決サーバは、名前解決データベース (図14 (b) 参照) を更新 (S582) して、更新完了通知を更新対象ドメインホームサーバに送信する。更新対象ドメインホームサーバは、さらに、自己の管理ユーザデバイスであるエンドエンティティである更新対象ドメイン内EEに対して、更新された新アドレスを通知 (S583) し、更新対象ドメイン内EEにおいて、新アドレスに基づくアドレス更新が実行 (S584) されて、更新完了通知が更新対象ドメインホームサーバに通知され、更新処理が終了する。

【0259】

図38を参照してアドレス更新による効果について説明する。図38のユーザデバイス3 21がアクセス元EEであり、ユーザデバイス311がアクセス先EEである。ユーザデ 50

バイス 3 2 1 (アクセス元 E E) は、ユーザデバイス 3 1 1 (アクセス先 E E) からアクセス許可グループのメンバーとして、過去において、認められていたが、現在はアクセス許可グループのメンバーから除外されているものとする。

【0 2 6 0】

たとえば、ユーザデバイス 3 2 1 (アクセス元 E E) のドメイン名 [home 2. x y z. c o m] がアクセス許可グループとして、ユーザデバイス 3 1 1 (アクセス先 E E) を管轄する中継サーバ 1 (ホームサーバ 1) 3 1 3 の適用する許可グループデータベース 3 1 4 に登録されていたが、その後削除されたものとする。さらに、ユーザデバイス 3 1 1 (アクセス先 E E) は、前述した説明に従ったアドレス更新を実行して、旧アドレス [1 0. 0. 1. 1 0 0] から、新アドレス [1 0. 0. 1. 2 2 2] に更新処理を行なった 10 10

【0 2 6 1】

ユーザデバイス 3 2 1 (アクセス元 E E) は、過去にユーザデバイス 3 1 1 (アクセス先 E E) にアクセスした時点で取得したアドレス [1 0. 0. 1. 1 0 0] を適用して、ユーザデバイス 3 1 1 (アクセス先 E E) に対するアクセスを実行しようとしても、現在のユーザデバイス 3 1 1 (アクセス先 E E) のアドレスは新アドレス [1 0. 0. 1. 2 2 2] であるので、アクセスすることはできない。

【0 2 6 2】

また、ユーザデバイス 3 1 1 (アクセス先 E E) のホスト名 [e e - a. h o m e 1. a b c. n e t] を適用して名前解決処理によって新アドレスを取得してアクセスを実行しようとしても、中継サーバ 1 (ホームサーバ 1) 3 1 3 における属性証明書検証および審査により、ユーザデバイス 3 2 1 (アクセス元 E E) は、ユーザデバイス 3 1 1 (アクセス先 E E) からアクセス許可グループのメンバーとして認められていないと判断され、名前解決処理が拒否されることになり、新アドレスの取得が行なわれず、新アドレスによるアクセスの実行は防止される。 20

【0 2 6 3】

〔(4) 各エンティティの構成〕

次に、上述した処理、すなわち属性証明書の生成、検証、送受信等を実行するユーザデバイスとしてのエンドエンティティ (E E)、中継サーバとしてのホームサーバ、あるいはサービスプロバイダ (S P) 等、各エンティティの情報処理装置としての構成例について 30 30 図を参照しながら、説明する。

【0 2 6 4】

ユーザデバイス、ホームサーバ、サービスプロバイダ等、各エンティティの情報処理装置は、各種のデータ処理、および制御を実行する C P U を有し、かつ他エンティティと通信可能な通信手段を備えた例えば、サーバ、P C、P D A、形態通信端末装置等の各種の情報処理装置によって構成可能である。

【0 2 6 5】

図 3 9 に情報処理装置構成例を示す。なお、図 3 9 に示す構成例は 1 つの例であり、各エンティティは、ここに示すすべての機能を必ずしも備えることが要求されるものではない。 40 40 図 3 9 に示す C P U (Central processing Unit) 9 5 1 は、各種アプリケーションプログラムや、O S (Operating System) を実行するプロセッサである。R O M (Read-Only-Memory) 9 5 2 は、C P U 9 5 1 が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。R A M (Random Access Memory) 9 5 3 は、C P U 9 5 1 の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

【0 2 6 6】

H D D 9 5 4 はハードディスクの制御を実行し、ハードディスクに対する各種データ、プログラムの格納処理および読み出し処理を実行する。セキュリティチップ 9 6 2 は、前述したように耐タンパ構造を持つ構成であり、暗号処理に必要な鍵データ等を格納し、権限 50 50

確認処理としての属性証明書の検証、あるいは生成処理等を実行する暗号処理部、データ処理部、メモリを有する。

【0267】

バス960はPCI (Peripheral Component Interface) バス等により構成され、各モジュール、入出力インタフェース961を介した各入力装置とのデータ転送を可能にしている。

【0268】

入力部955は、例えばキーボード、ポインティングデバイス等によって構成され、CPU951に各種のコマンド、データを入力するためにユーザにより操作される。出力部956は、例えばCRT、液晶ディスプレイ等であり、各種情報をテキストまたはイメージ等により表示する。 10

【0269】

通信部957はデバイスの接続したエンティティ、例えばサービスプロバイダ等との通信処理を実行するネットワークインタフェース、接続機器インタフェース等からなり、CPU951の制御の下に、各記憶部から供給されたデータ、あるいはCPU951によって処理されたデータ、暗号化されたデータ等を送信したり、他エンティティからのデータを受信する処理を実行する。

【0270】

ドライブ958は、フレキシブルディスク、CD-ROM (Compact Disc Read Only Memory)、MO (Magnetooptical) ディスク、DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体959の記録再生を実行するドライブであり、各リムーバブル記録媒体959からのプログラムまたはデータ再生、リムーバブル記録媒体959に対するプログラムまたはデータ格納を実行する。 20

【0271】

各記憶媒体に記録されたプログラムまたはデータを読み出してCPU951において実行または処理を行なう場合は、読み出したプログラム、データはインタフェース961、バス960を介して例えば接続されているRAM953に供給される。

【0272】

前述の説明内に含まれるユーザデバイス、サービスプロバイダ等における処理を実行するためのプログラムは例えばROM952に格納されてCPU951によって処理されるか、あるいはハードディスクに格納されHDD954を介してCPU951に供給されて実行される。 30

【0273】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0274】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。 40

【0275】

例えば、プログラムは記録媒体としてのハードディスクやROM (Read Only Memory) に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD-ROM (Compact Disc Read Only Memory)、MO (Magnetooptical) ディスク、DVD (Digital V 50

ersatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納(記録)しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

【0276】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【0277】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【0278】

【発明の効果】

以上、説明したように、本発明によれば、通信ネットワークを介した通信処理装置間の通信において、アクセス先の許容するアクセス元であるか否かをホームサーバ等の中継サーバにおいて判定して、アクセス先の許容するアクセス元である場合にのみ、名前解決処理を実行して、アクセス先のアドレス情報をアクセス元に通知する構成としたので、アクセス先の許容したアクセス元からのアクセスのみを実行する構成が実現される。

【0279】

さらに、本発明の構成によれば、通信ネットワークを介した通信処理装置間の通信において、ホームサーバ等の中継サーバが、アクセス元の属性証明書の検証、審査を実行して、アクセス元がアクセス先の許容メンバーであるか否かの判定処理を実行し、アクセス先の許容するアクセス元である場合にのみ、名前解決処理を実行して、アクセス先のアドレス情報をアクセス元に通知する構成としたので、属性証明書に基づく確実な審査によるアクセス制限を実行することが可能となる。

【0280】

さらに、本発明の構成によれば、アクセス元のドメイン名属性証明書、ホスト名属性証明書等、属性情報としてドメイン名、ホスト名を記述したグループ属性証明書を適用する構成としたので、特定ドメインに属する機器、あるいは特定ホスト名の機器に限定したアクセス制限を実行することが可能となる。

【0281】

さらに、本発明の構成によれば、アクセス元のドメイン名属性証明書、ホスト名属性証明書等、属性情報としてドメイン名、ホスト名を記述したグループ属性証明書を適用する構成とするとともに、ドメイン名、ホスト名に対応するアドレスの更新を実行する構成としたので、旧アドレスを適用したアクセスの排除が可能となる。

【図面の簡単な説明】

【図1】 アクセス権限管理システムにおける公開鍵基盤、権限管理基盤構成について説明する図である。

【図2】 公開鍵証明書のフォーマットを示す図である。

【図3】 公開鍵証明書のフォーマットを示す図である。

【図4】 公開鍵証明書のフォーマットを示す図である。

【図5】 権限情報証明書としての属性証明書のフォーマットを示す図である。

【図6】 グループ属性証明書(グループAC)の構成例を示す図である。

【図7】 ドメイン名属性証明書およびホスト名属性証明書のフォーマットを示す図である。

。

【図8】 ドメイン名属性証明書の発行体系を説明する図である。

【図9】 ホスト名属性証明書の発行体系を説明する図である。

10

20

30

40

50

【図10】アクセス権管理システムに参加する各エンティティの信頼関係構成を説明するトラストモデルを示す図である。

【図11】ユーザデバイス、ホームサーバ、サービスプロバイダ等のエンティティに構成されるセキュリティチップの構成例を示す図である。

【図12】ユーザデバイスのセキュリティチップの格納データ例を示す図である。

【図13】アクセス権管理システムの概要について説明する図である。

【図14】名前解決サーバの有するデータベース構成例である。

【図15】ドメイン名登録処理シーケンスを示す図である。

【図16】ドメイン名属性証明書発行処理シーケンスを示す図である。

【図17】公開鍵暗号方式の1つの認証処理方式であるハンドシェイクプロトコル (T L S 1. 0) について示す図である。

【図18】メッセージ認証コード: MAC (Message Authentication Code) の生成構成を示す図である。

【図19】電子署名の生成処理を説明するフロー図である。

【図20】電子署名の検証処理を説明するフロー図である。

【図21】新規エンドエンティティ (E E) の登録処理シーケンスを示す図である。

【図22】エンドエンティティ (E E) によるドメイン名属性証明書発行処理シーケンスを示す図である。

【図23】エンドエンティティ (E E) によるホスト名属性証明書発行処理シーケンスを示す図である。

【図24】エンドエンティティ (E E) によるアクセス許可グループ情報登録処理シーケンスを示す図である。

【図25】アクセス許可グループ情報のデータ構成例を示す図である。

【図26】エンドエンティティ (E E) によるアクセス許可グループ情報削除処理シーケンスを示す図である。

【図27】アクセス権限の確認を伴うアクセス処理シーケンスを説明する図である。

【図28】ドメイン名に基づくアドレス取得処理シーケンスを説明する図である。

【図29】公開鍵証明書 (P K C) と属性証明書 (A C) との関連について説明する図である。

【図30】属性証明書 (A C) の検証処理フローを示す図である。

【図31】公開鍵証明書 (P K C) の検証処理フローを示す図である。

【図32】アクセス権限審査処理について説明するシーケンス図である。

【図33】アクセス権限の確認を伴うアクセス処理シーケンスを説明する図である。

【図34】エンドエンティティ (E E) のアドレス更新処理シーケンスを示す図である。

【図35】エンドエンティティ (E E) のアドレス空間更新処理シーケンスを示す図である。

【図36】ドメインに対応するアドレス空間の更新処理シーケンスを示す図である。

【図37】ドメインに対応するアドレスの更新処理シーケンスを示す図である。

【図38】アドレスの更新処理による効果を説明する図である。

【図39】ユーザデバイス、ホームサーバ、サービスプロバイダ等、各エンティティの情報処理装置構成例を示す図である。

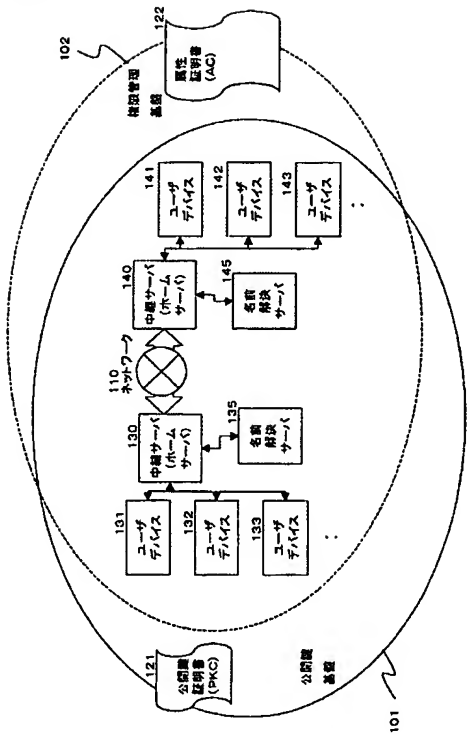
【符号の説明】

- 101 公開鍵基盤
- 102 権限管理基盤
- 110 ネットワーク
- 121 公開鍵証明書
- 122 属性証明書
- 130, 140 中継サーバ (ホームサーバ)
- 131-133, 141-143 ユーザデバイス
- 135, 145 名前解決サーバ

150	ドメイン名属性証明書認証局	
151, 152, 153	ドメイン領域	
154	セカンドレベルドメイン割当機関	
155	サービスプロバイダ	
156, 157	ホームサーバ	
158-160	エンドエンティティ (EE)	
161-166	ドメイン名属性証明書	
171, 172	ホスト名属性証明書認証局	
173-177	ホスト名属性証明書	
180	システムホルダ	10
181	ルート認証局 (CA)	
182	認証局 (CA)	
183	登録局 (RA)	
184	属性証明書認証局 (AA)	
185	属性証明書登録局 (ARA)	
186	ポリシーテーブル	
187	サービスプロバイダ (SP)	
190	ドメイン領域	
191	エンドエンティティ (EE)	
192	ホームサーバ (HS)	20
200	デバイス	
201	CPU (Central processing Unit)	
202	インタフェース	
203	ROM (Read-Only-Memory)	
204	RAM (Random Access Memory)	
205	暗号処理部	
206	メモリ部	
210	セキュリティチップ	
221	ユーザデバイス側制御部	
222	外部メモリ部	30
231	接続機器インタフェース	
232	ネットワークインタフェース	
311, 321	ユーザデバイス	
312, 322	名前解決サーバ	
313, 323	中継サーバ (ホームサーバ)	
314, 324	許可グループデータベース	
331, 341	サービスプロバイダ	
332, 342	ドメイン名属性証明書登録局	
333, 343	名前解決サーバ	
351, 352	ドメイン名属性証明書認証局	40
355	通信ネットワーク	
951	CPU (Central processing Unit)	
952	ROM (Read-Only-Memory)	
953	RAM (Random Access Memory)	
954	HDD	
955	入力部	
956	出力部	
957	通信部	
958	ドライブ	
959	リムーバブル記録媒体	50

- 9 6 0 バス
- 9 6 1 入出力インタフェース
- 9 6 2 セキュリティチップ

【図 1】



【図 2】

Ver sion	項目	説明
V-1	version	証明書のフォーマットのバージョン
	serialNumber	証明書発行者によって割り当てられる証明書番号
	signature	証明書の署名アルゴリズム
	issuer	証明書の発行者 (Distinguished Name 形式)
	validity notBefore notAfter	証明書の有効期限 開始日時 終了日時
	subject	証明書の所有者
	subjectPublicKeyInfo algorithm subjectPublicKey	証明書の所有者の公開鍵情報 アルゴリズム 公開鍵

【図 3】

V-3	authorityKeyIdentifier keyIdentifier authorityCn authorityCnSerialNumber	署名検証に用いる証明書発行者の識別子 識別子 識別証明書の発行番号(Certificate Number) 識別証明書のシリアル番号
	subjectKeyIdentifier keyIdentifier	署名の属の中から目的の属を明確に識別
	key usage (0)digitalSignature (1)nonRepudiation (2)keyEncipherment (3)dataEncipherment (4)keyAgreement (5)keyCertSyn (6)RLSign privateKeyUsagePeriod notBefore notAfter	属の使用目的を指定 (0)デジタル署名用 (1)否認防止用 (2)属の暗号化用 (3)メッセージの暗号化用 (4)共通鍵暗号化用 (5)認証書の署名生成用 (6)失効リストの署名生成用 証明書中の公開鍵に対応する秘密鍵の有効期間
	certificatePolicies policyIdentifier policyQualifiers	証明書発行者が適用した証明書ポリシー ポリシーID(ISO/IEC9894-1:1996) 認証基準
	policyMappings issuerDomainPolicy subjectDomainPolicy	認証基準中のポリシーの関係を制御 (CA証明書にのみ必要)

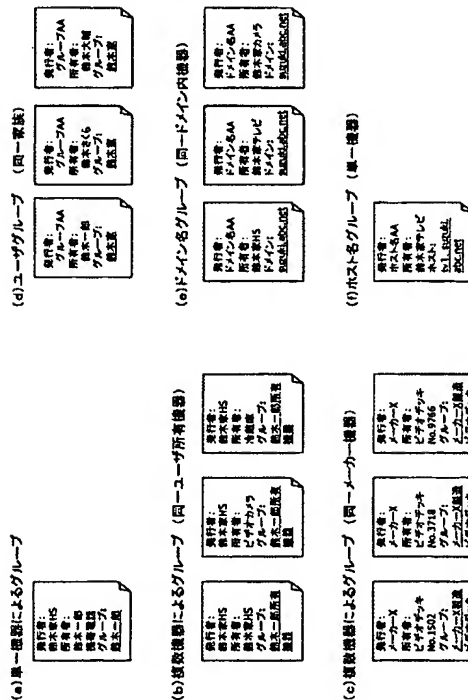
【図 4】

V-3	subjectAltName	証明書所有者の署名 (GN形式)
	issuerAltName	証明書発行者の署名 (GN形式)
	subjectDirectoryAttributes	証明書所有者のために必要とされるディレクトリの属性
	basicConstraints ca pathLenConstraint	証明書の公開鍵が認証の署名所か、証明書所有者のものかを区別
	nameConstraints permittedSubtrees base inhibitAnyPolicy excludedSubtrees	発行者が発行する証明書の名前を制御
	policyConstraints requireExplicitPolicy inhibitPolicyMapping	認証基準中のポリシーの関係を制御
	crlDistributionPoints	証明書所有者が証明書を利用する際に、証明書が失効していないかどうかを確認するための失効リストの参照点を記述
	signatureAlgorithm	証明書への署名付けに用いるアルゴリズム
	signatureValue	証明書発行者の秘密鍵による署名

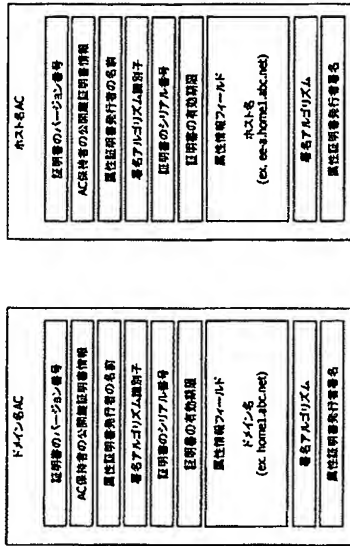
【図 5】

グループ属性証明書 (AC: Attribute Certificate)	
証明書のバージョン番号	
AC保持者の公開鍵証明情報	
属性証明書発行者の名前	
署名アルゴリズム識別子	
証明書のシリアル番号	
証明書の有効期限	
属性情報フィールド グループID、または、 ドメイン名、または、 ホスト名など	
署名アルゴリズム	
属性証明書発行者署名	

【図 6】



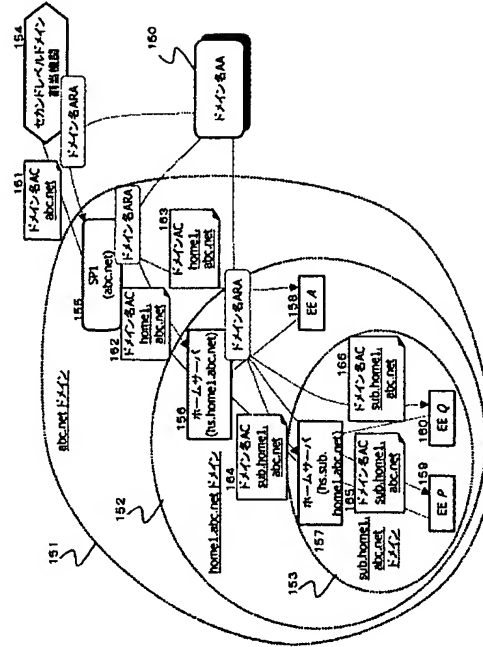
【図 7】



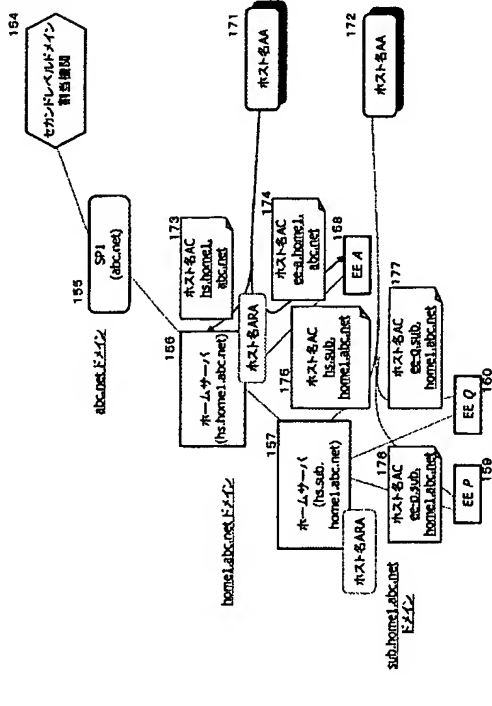
(f)

(a)

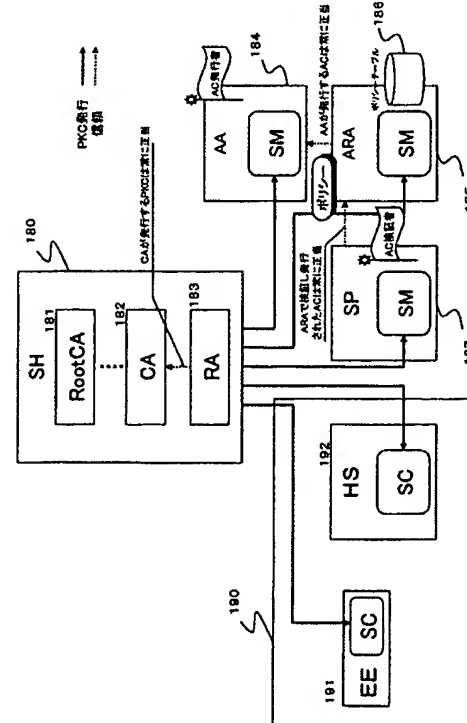
【図 8】



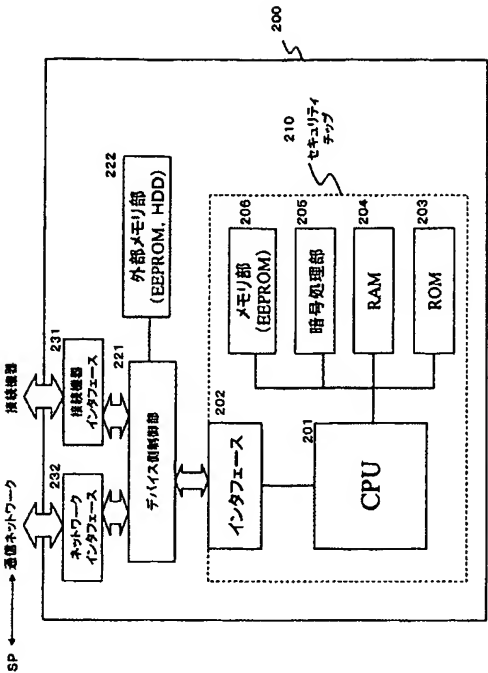
【図 9】



【図 10】



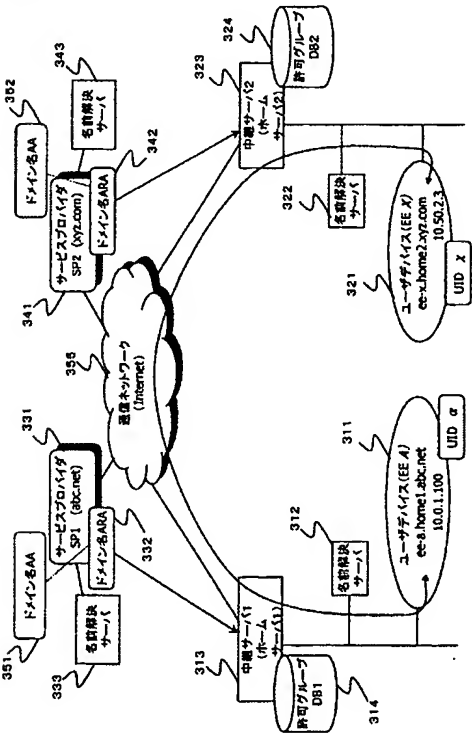
【図 1 1】



【図 1 2】

データ種別	データ内容
公開鍵証明書	・ルート証明書公開鍵証明書 ・サブ証明書公開鍵証明書
グループ属性証明書	・秘密鍵の属するまたはユーザの属するグループ対応の属性証明書
鍵データ	・セキュリティチップ公開鍵、秘密鍵ペア ・乱数生成用鍵、相互認証用鍵
追加情報	・セキュリティチップID ・サブ証明書ID ・ユーザID ・アプリケーションID
その他	・乱数シード(Seed) ・サブサービス情報等

【図 1 3】



【図 1 4】

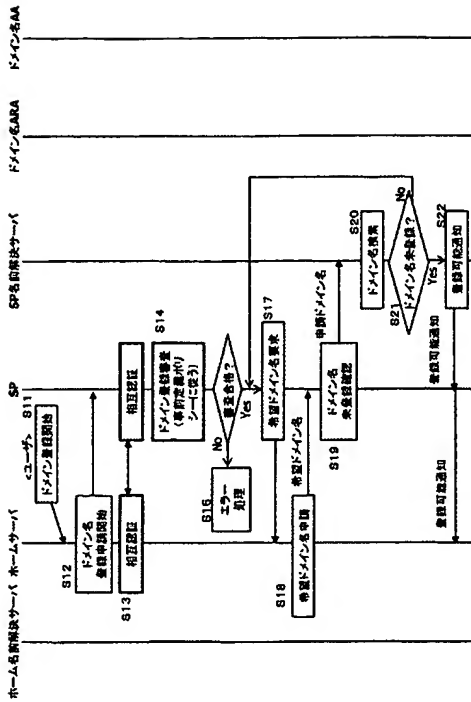
ドメイン名	アドレス空間	ホームサーバIPアドレス
home1.abc.net	10.0.1.1-255	10.0.1.5
home2.abc.net	10.0.2.1-255	10.0.2.1
office100.abc.net	10.0.100.1-255	10.0.100.251
nameserver-xyz.com	—	10.50.0.1

(a)

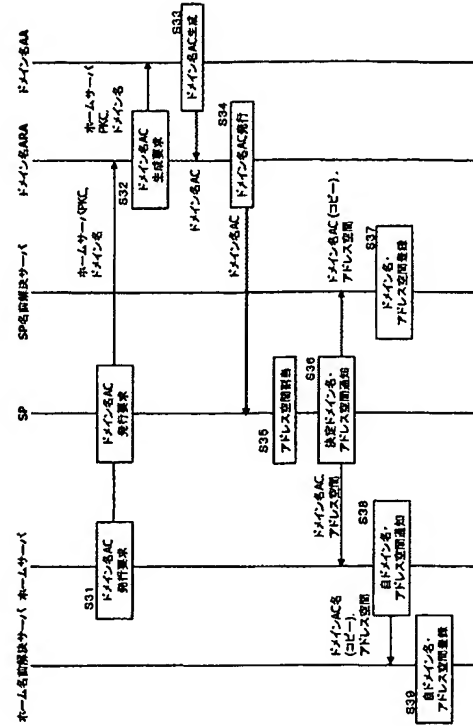
ホスト名	IPアドレス
ee-a.home1.abc.net	10.0.1.100
ee-b.home1.abc.net	10.0.1.150
nameserver.abc.net (SP1名解決サーバ)	10.0.0.1

(b)

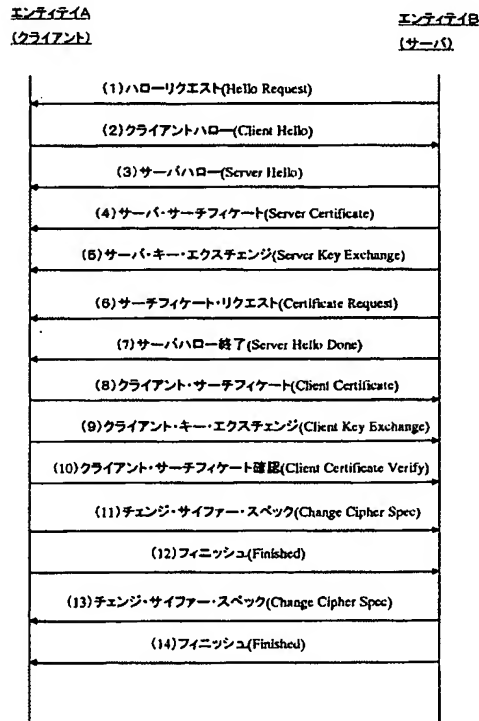
【図 15】



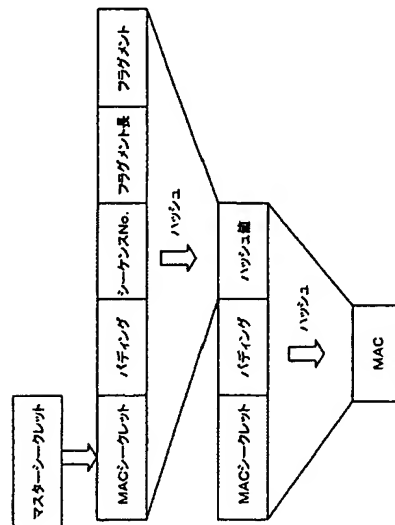
【図 16】



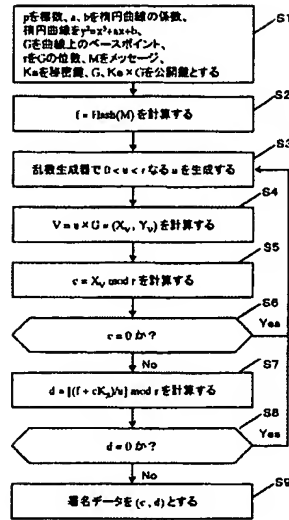
【図 17】



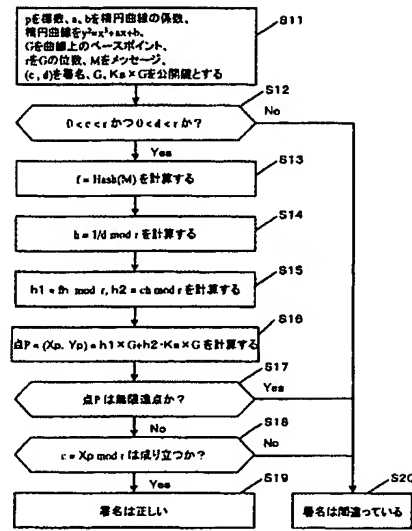
【図 18】



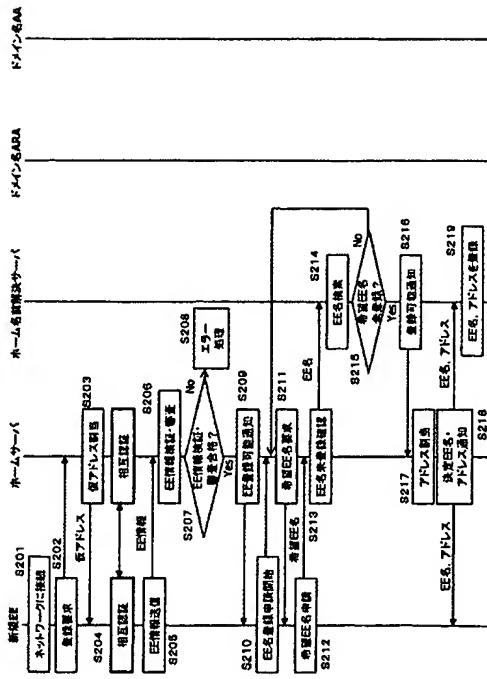
【図 19】



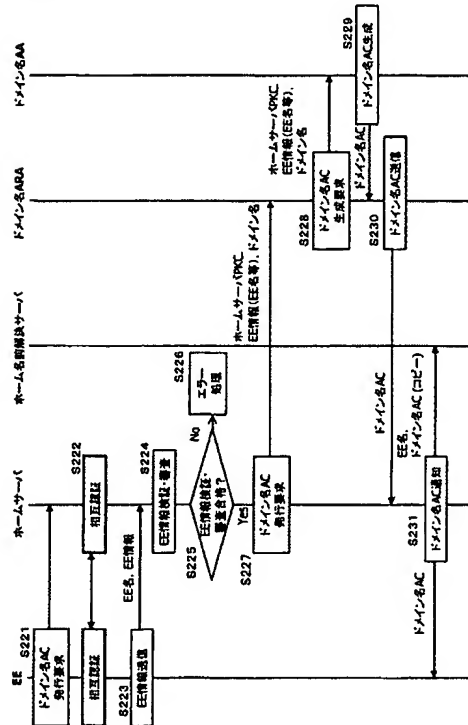
【図 20】



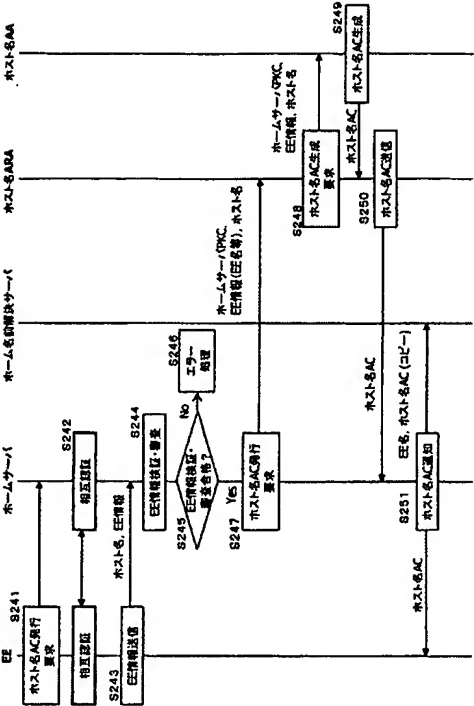
【図 21】



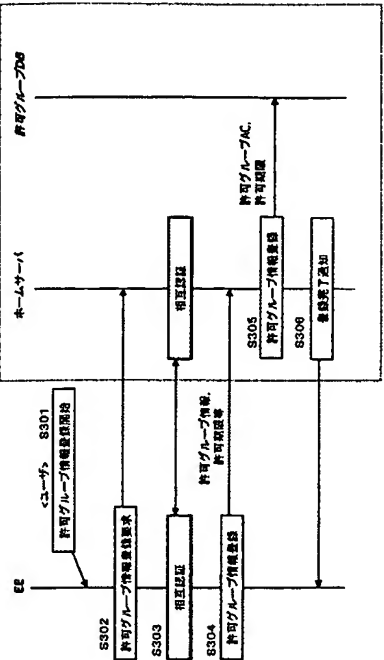
【図 22】



【図 2 3】



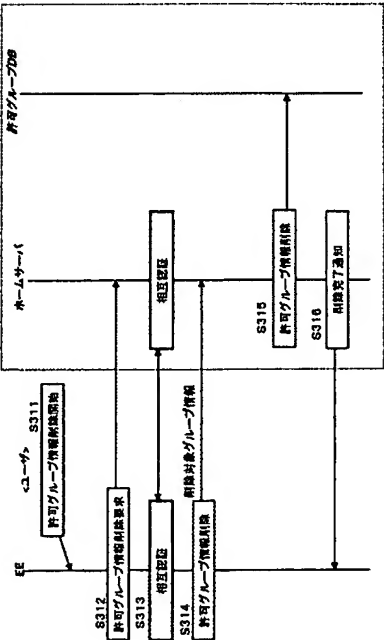
【図 2 4】



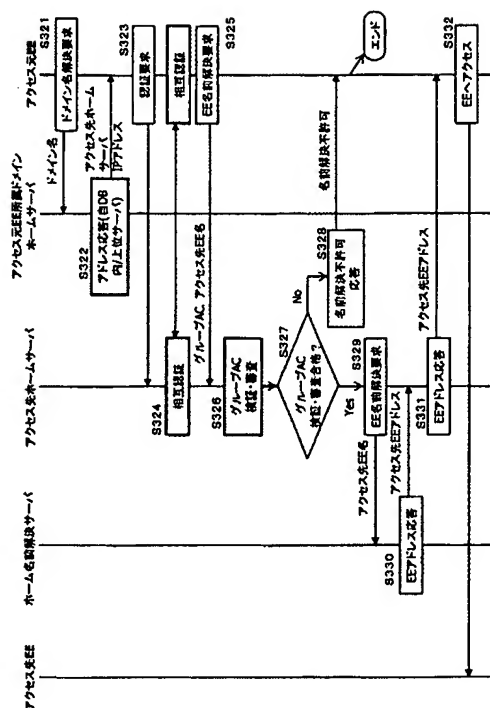
【図 2 5】

EE名	アクセス許可グループ	許可期限
ee-a	A社所属機器, ユーザ	5月5日
ee-a	鈴木 太郎, ユーザ	無期限
ee-a	abc.net ドメイン内機器	48時間
ee-b	A社アメリカ支店機器, ユーザ	AC有効期限内
ee-b	X大学理学部 機器, ユーザ	3月31日
ee-b	ee-home2abc.net	4月8日
ee-b	ホスト機器	

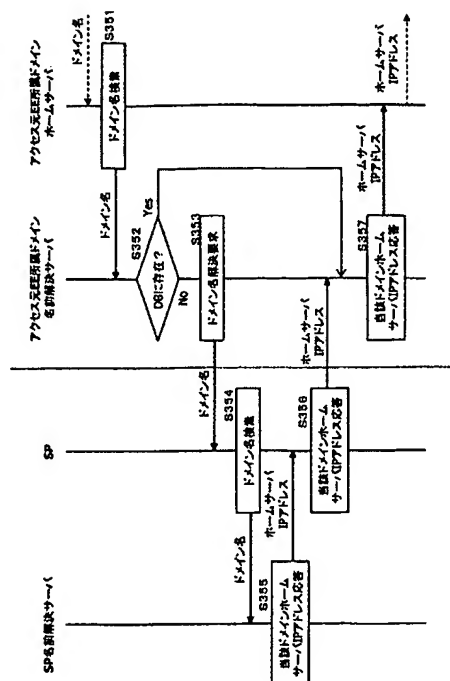
【図 2 6】



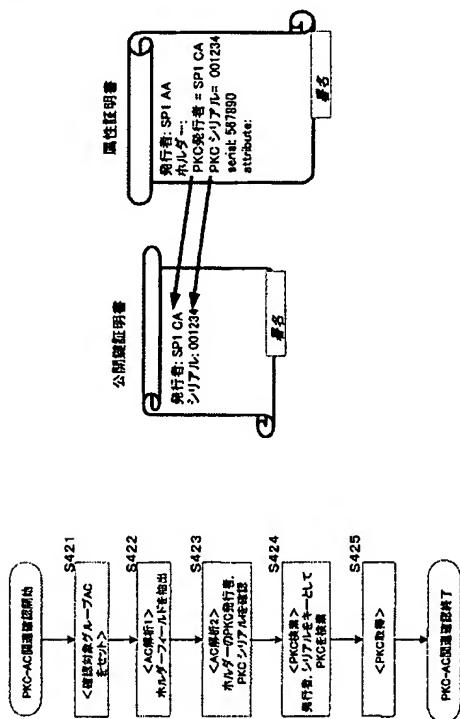
【图 27】



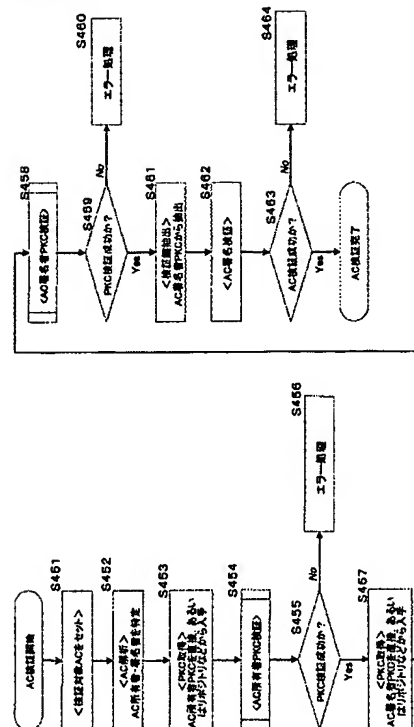
【図 28】



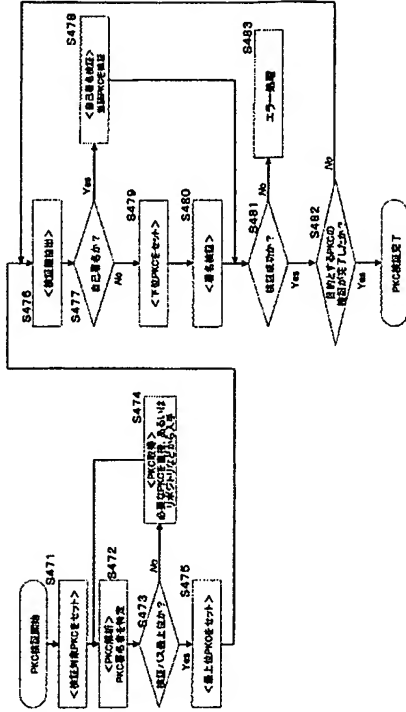
【图 29】



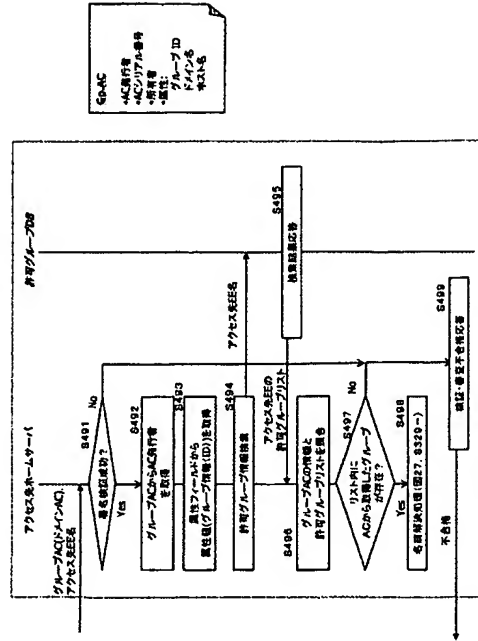
【図 30】



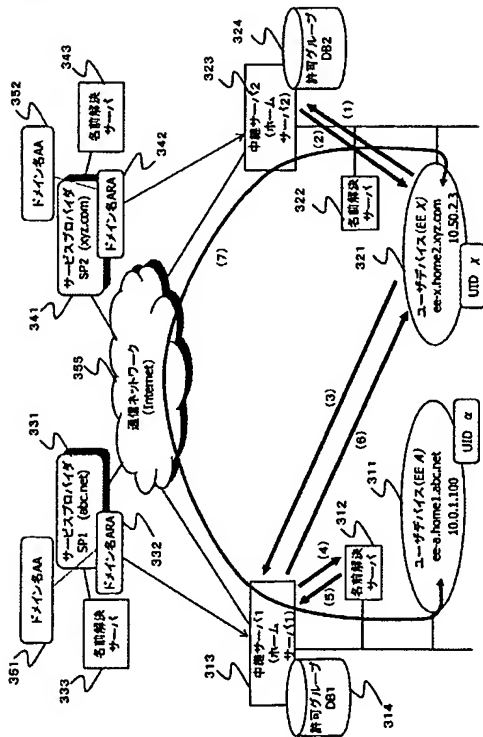
【図 31】



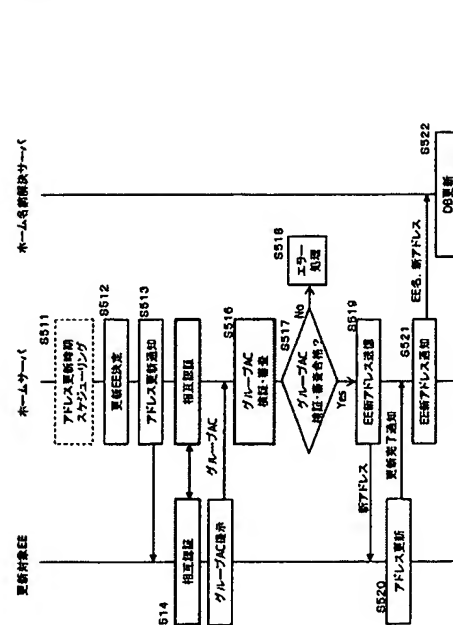
【図 32】



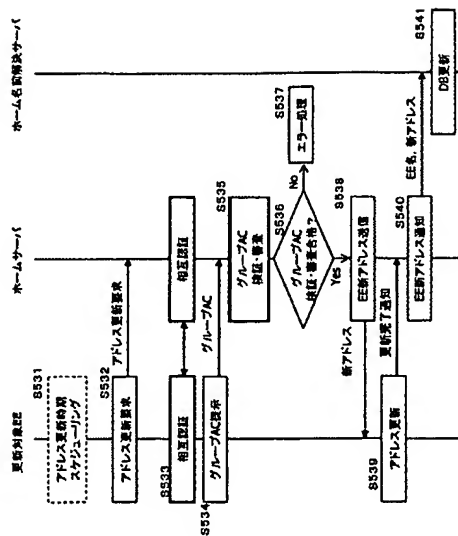
【図 33】



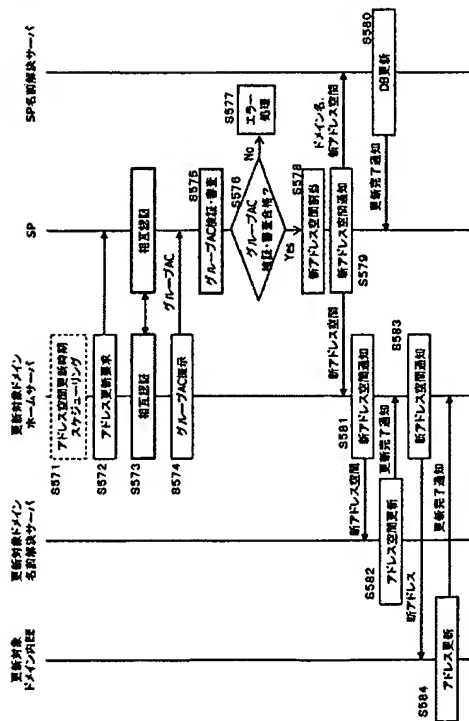
【図 34】



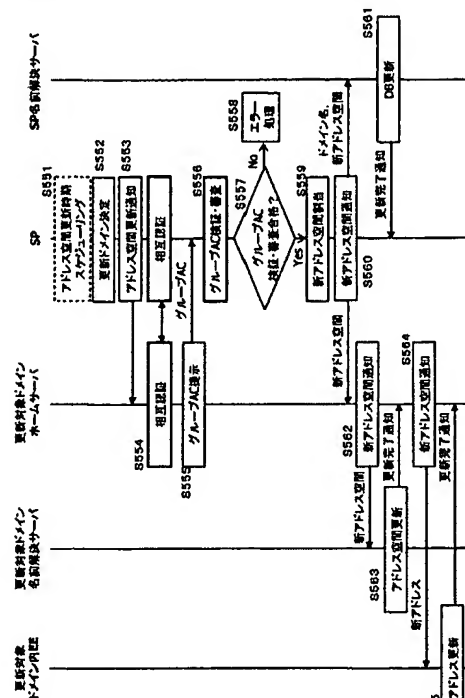
【図 35】



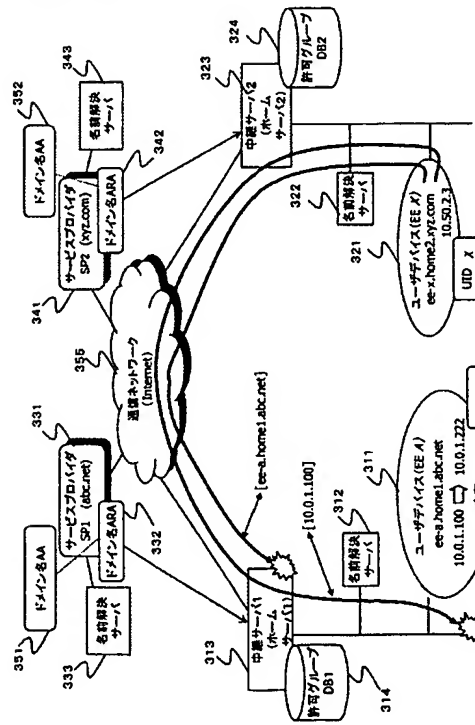
【図 3 7】



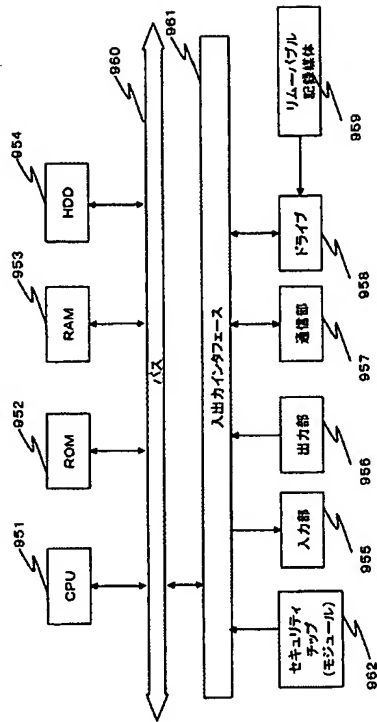
【図 3 6】



【図 38】



【図 39】



フロントページの続き

(51)Int.Cl.

F I

テーマコード (参考)

H 0 4 L 12/56

H 0 4 L 12/56 B

H 0 4 L 9/00 6 7 5 B

(72)発明者 川口 貴義

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 間杉 円

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 石橋 義人

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 阿部 博

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 豊島 信隆

東京都品川区北品川6丁目7番35号 ソニー株式会社内

F ターム (参考) 5B085 AE02 AE04 BC02

5J104 AA07 AA08 AA09 EA30 JA21 JA25 KA02 KA05 LA01 LA03

LA06 MA01 NA02 NA12

5K030 GA15 HA08 HC01 HD03 HD06 HD09 KA07 LD20

5K033 AA08 CB01 CB08 DA06 DB12 DB14 DB16 DB18 EC03